

Receptor de estados cuánticos codificados en la fase óptica de pares de pulsos. Estabilización de un interferómetro con desbalance de caminos

JULIA BERTERO DI TELLA

Director: DR. MIGUEL A. LAROTONDA

Tesis de licenciatura en Ciencias Físicas
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Diciembre de 2024

TEMA: Receptor de estados cuánticos codificados en la fase óptica de pares de pulsos. Estabilización de un interferómetro con desbalance de caminos.

ALUMNA: Julia Bertero Di Tella

L.U: 285/19

LUGAR DE TRABAJO: Laboratorio de Óptica Cuántica, DEILAP, UNIDEF.

DIRECTOR DEL TRABAJO: Dr. Miguel A. Larotonda

FECHA DE INICIACIÓN: Agosto 2023

FECHA DE FINALIZACIÓN: Diciembre 2024

FECHA DE EXAMEN:

INFORME FINAL APROBADO POR:

Autora: Julia Bertero Di Tella

Jurado

Director: Dr. Miguel A. Larotonda

Jurado

Profesora de Tesis de Licenciatura

Jurado

Resumen

En este trabajo se detalla la estabilización en temperatura de un interferómetro de Mach-Zehnder utilizado para experimentos de Distribución Cuántica de Claves. Se diseñó e implementó un control de temperatura basado en el componente MAX1979. Primero se caracterizó la estabilidad de un láser de 1550 nm utilizado como fuente del interferómetro y se encontró que para tiempos menores a 30 s su frecuencia es estable en 0.1 ppm. Luego se caracterizó el control de temperatura y se lo utilizó para estabilizar térmicamente el interferómetro. Fue posible estabilizar el mismo para que la temperatura fluctúe menos de 50 mK. Luego se utilizó un lazo de control sobre un *fiber stretcher* que regula el desbalance óptico del interferómetro, con el que fue posible estabilizar la fase por al menos 50 minutos. Se logró un contraste de (0.985 ± 0.013) . Se halló que el contraste del interferómetro varía con la temperatura. Finalmente se utilizó dicho interferómetro para generar dos pulsos *time-bin*. Esta última etapa se centró en estudiar y optimizar el método ya implementado en el laboratorio de generación de pulsos. Usando una frecuencia de reloj $f_{GPP} = 480$ MHz, se obtuvo un patrón de pares de pulsos con separación temporal de $\Delta t = 2.2$ ns. Se pudieron generar dos estados con $\Delta\varphi = 0$ y $\Delta\varphi = \pi$, donde el contraste fue de (0.9512 ± 0.0064) . Se observó que el contraste cambia entre mediciones de luz intensa y de conteo, y se conjetura que esta variación es debida a efectos de birrefringencia inducidos térmicamente

Agradecimientos

La verdad que no se como llegue hasta acá, todavía no caigo que estoy escribiendo la tesis y acá estoy a nada de entregarla. No hubiese llegado hasta acá sin mis amigos y todos los que me acompañaron estos últimos años. Quiero agradecerle a mi director, Richi por toda su ayuda en este proceso y también por todo el apoyo y los consejos que me diste todo este último tiempo. Gracias por darme la oportunidad de hacer la tesis con vos y de formar parte por este tiempito del hermoso equipo que hay en el laboratorio. Gracias por toda la ayuda con la tesis y también todos los consejos con respecto al futuro y por responder siempre todas mis dudas. Gracias también a Julián por todas las risas en Bariloche y en el labo todos los días, se te extraña. Gracias por estar siempre y ayudarme con mis dudas de la tesis y siempre estar para conversar. Gracias a Agus, a quien admiro muchísimo y siempre fue una inspiración, gracias por toda tu ayuda, por guiarme en mi busca de doc y por introducirme a la tribu. Gracias a Pili por hacerme sentir bienvenida en el labo y por alegrar cada día que vengo al Citedef. A Lau, por hacerme sentir bienvenida y cómoda en el laboratorio, por toda tu ayuda y tu apoyo siempre. Gracias también a Tute, Jorge y Marce por todo el apoyo, por hacer que cada día en el labo sea más divertido y por todas las charlas compartidas.

Gracias también a Christian, por ser un gran director de labo 6y7, por todo lo que me enseñaste y por guiarme en el laboratorio y por darme la oportunidad de formar parte del LIAF. Mi paso por el laboratorio fue una experiencia muy linda y gracias a eso decidí que quería seguir un doctorado. Gracias a todo el equipo del LIAF, a Muri, Nico, Lio y Lauti por haber hecho de mi primer experiencia en un labo una experiencia muy linda. Gracias por todo, no estaría acá sin su apoyo, gracias por hacerme sentir menos perdida en el labo y por hacerme sentir bienvenida. Gracias a Muri en especial por tus consejos en el CUANTOS cuando entre en crisis porque no entendía ninguna charla, gracias por hacerme sentir menos sola y por insistirme que aplique a la beca de Optica. Gracias también a Jean Paul, no estaría acá si no fuese por vos, gracias por decidir de hacer labo 6y7 conmigo cuando apenas nos conocíamos, por todas las charlas en el labo y por tu paciencia. Gracias también a Sebas que desde que nos conocimos mas en Bariloche siempre fue un gran apoyo y por todas las charlas.

A mis amigos que me acompañan desde el CBC, Mori, Lula, Delfi, Fede y Tomi, gracias por todo su apoyo, los quiero mucho, realmente no hay palabras de lo agradecida que estoy de

que estén en mi vida. Gracias por todas las veces que me apoyaron y me escucharon quejarme de un parcial o una clase, realmente no hubiese llegado hasta acá si no fuese por ustedes. Gracias a Mori por todas las charlas a lo largo de los años, por escuchar todas mis crisis con la carrera y siempre estar para mí, por todas las risas, las jodas y los tiempos compartidos. Gracias a Fede, que ya sos como un hermano, por todo el apoyo a lo largo de los años, gracias por bancarme en mis locuras y estrés, por todas las veces que me compraste cafe y por cuidar a cochi aunque este loca. Gracias Delfi, por todas las charlas en especial en la pandemia y por el apoyo moral para seguir con el delirio de 10hs de clase por día, sin vos no sobrevivía ese año. Gracias Tomi, por bancarme desde el segundo día del CBC cuando te conocí con Fede, por siempre estar y por ayudarnos a estar más tranquila y no enojarte cuando en labo 5 pasabamos horas estresadas con Delfi por los informes. Gracias a Lula por estar ahí cuando te necesito, por ser siempre honesta y por empujarme cuando lo necesito, valoro muchísimo tu amistad. Gracias a Juli, estoy eternamente agradecida de habernos conocido y de ser amigas, en los últimos dos años te volviste una de las personas más importantes en mi vida, te quiero muchísimo. Gracias por hacerme sentir menos sola y por estar siempre y ayudarme cada vez que sentía que estaba haciendo todo mal con la tesis. Gracias también a Ine por tu amistad y todo tu apoyo, por estar siempre, por mas juntadas de verano a tomar mates, te quiero. No hay suficientes páginas para expresar lo mucho que los quiero pero quiero que sepan lo mucho que significan para mi y lo agradecida que estoy de ser su amiga. Gracias también a todos los amigos que me hice durante estos años en la facu, en especial a Ana, Luchi, Nico, Willy y Joaco Cullen, por todos los mates, las charlas y las juntadas.

Gracias a Cande, mi amiga de hace mas de 10 años, mi compa de jodas y casi tan adicta al café como yo, gracias por siempre estar en mis mejores y peores momentos, por escuchar mis mil audios eternos y bancarme en todas, te quiero mucho. Gracias también a Mariano, Euge y Tizi, por escucharme hablar de física, por todas las meriendas y conversaciones de estos últimos años, los quiero.

Por último gracias a mi familia por darme la oportunidad de estudiar y apoyarme en el proceso, en especial a Clari y a mi mamá por escucharme y ayudarme cada vez que me estresé por un parcial y por estar siempre, las quiero mucho.

Gracias a la facultad por todo lo que aprendí y la gente que conocí. Por todas las oportunidades que me dió como trabajar en tecnópolis donde crecí y me di cuenta de cuanto me gusta la divulgación. Gracias a la Universidad pública por permitirme estudiar esta hermosa carrera.

Índice general

| | |
|--|-----------|
| 1. Introducción | 1 |
| 1.1. Historia de la criptografía | 1 |
| 1.2. Fundamentos de la teoría de la información cuántica | 4 |
| 1.2.1. Estados cuánticos, observables y evolución temporal | 4 |
| 1.2.2. Mediciones | 5 |
| 1.2.3. Qubits y bases conjugadas | 5 |
| 1.2.4. Teorema de no clonación de estado cuánticos | 6 |
| 1.3. Distribución Cuántica de Claves | 7 |
| 1.3.1. Protocolo BB84 | 8 |
| 1.3.2. Ataques y su detección | 9 |
| 1.4. Implementación física de los qubits | 10 |
| 1.4.1. Fuente de fotones | 11 |
| 1.4.2. Canal cuántico - fibras ópticas | 12 |
| 1.4.3. Modos temporales discretos de fotones: <i>time-bin</i> | 14 |
| 1.4.4. Detección | 18 |
| 1.5. Otras aplicaciones de las fibras ópticas | 19 |
| 1.5.1. Monitoreo de signos vitales usando sensores de fibras ópticas | 21 |
| 2. Interferometría de fuentes independientes | 24 |
| 2.1. Varianza de Allan | 24 |
| 2.2. Láseres ITLA | 26 |
| 2.2.1. Principio de funcionamiento | 26 |
| 2.2.2. Modos de uso | 27 |
| 2.2.3. Caracterización de estabilidad. | 27 |
| 2.3. Medición de estabilidad a partir de los batidos de dos láseres | 31 |
| 2.3.1. Interferencia de dos fuentes de luz independientes | 32 |
| 3. Interferometría de una única fuente en dispositivos de fibra óptica | 35 |
| 3.1. Montaje experimental interferómetro de Mach - Zehnder | 35 |
| 3.2. Fibras ópticas | 38 |
| 3.3. Estabilización del interferómetro Mach-Zehnder. | 39 |

| | | |
|-----------|--|-----------|
| 3.3.1. | Interferómetro balanceado. | 39 |
| 3.3.2. | Interferómetro con desbalance de caminos. | 41 |
| 3.4. | Lazo de estabilización por maximización de intensidad. | 43 |
| 3.4.1. | Implementación del algoritmo de maximización. | 44 |
| 3.4.2. | Contraste y temperatura. | 45 |
| 3.5. | Control de temperatura | 47 |
| 3.5.1. | Diseño e implementación | 47 |
| 3.5.2. | Caracterización | 51 |
| 3.5.3. | Ecuación de Steinhart & Hart | 52 |
| 3.5.4. | Caracterización sobre el interferómetro. | 55 |
| 4. | Aplicación a QKD | 57 |
| 4.1. | Implementación experimental de protocolo de QKD en fibra óptica. | 57 |
| 4.2. | Caracterización del interferómetro con una fuente de pocos fotones | 60 |
| 4.2.1. | Optimización de generación de pulsos. | 60 |
| 4.2.2. | Generación de un segundo estado <i>time-bin</i> | 64 |
| 4.2.3. | Simulación de pulsos <i>time-bin</i> | 65 |
| 5. | Conclusiones | 69 |
| | Referencias | 71 |

Capítulo 1

Introducción

En la actualidad, la gran mayoría de los sistemas criptográficos es lo que se llama condicionalmente (o computacionalmente) segura. Pueden ser vulnerados pero en tiempos que exceden a la vida útil de la información cifrada. Sin embargo, con el desarrollo de nuevas tecnologías aparece la posibilidad de una computadora cuántica que, en caso de existir, volvería obsoletos los sistemas actuales de generación de claves ya que disminuiría significativamente el tiempo de cómputo. Como solución a este dilema aparece la Distribución Cuántica de Claves (QKD por sus siglas en inglés *Quantum Key Distribution*), que es capaz de lograr seguridad incondicional; es imposible de descryptar teóricamente. La característica principal de este protocolo es que se basa en fundamentos de la física cuántica, lo cual lo vuelve un protocolo de alta seguridad.

En este capítulo primero se presenta un resumen histórico del origen de la Distribución de Claves. Luego se introducen los fundamentos de la mecánica cuántica necesarios para su implementación y se presenta un ejemplo de un protocolo de encryptación conocido como BB84. Se detalla también como implementar experimentalmente este tipo de protocolos usando *qubits* codificados en los modos temporales discretos de la luz. El objetivo principal de este trabajo fue la estabilización en temperatura de un interferómetro de Mach-Zehnder en fibra óptica utilizado en los experimentos de QKD. Este tipo de interferómetros tienen múltiples aplicaciones más allá de la criptografía cuántica como elementos de sensado. Al final de este capítulo se detallan posibles usos de la fibra óptica y los interferómetros de Mach-Zehnder en sensado.

1.1 Historia de la criptografía

Las comunicaciones secretas existen ya hace varios siglos y sus orígenes se pueden rastrear a la civilización griega. Herodotus explica en su libro “Las historias” como la **esteganografía**; que se define como el arte de esconder mensajes para lograr comunicación secreta, salvó a Grecia de ser conquistada por los persas [1]. Un griego que había sido exiliado a Persia, notó que los

persas estaban planeando un ataque sorpresa y, como todavía mantenía lealtad con Grecia, decidió enviar una advertencia. Tomó tablas plegables de madera, les quitó la cera y escribió el mensaje que luego volvió a cubrir con cera de forma que a simple vista las tablas se veían blancas sin mensaje. Luego el receptor del mensaje le volvió a quitar la cera descubriendo así el mensaje escondido. El problema de enviar un mensaje secreto de esta forma es que cualquier persona que intercepte la tabla y le quite la cera descubrirá el mensaje. Es por esto que una vez descubierto este método no puede ser utilizado de nuevo.

A medida que se fueron descubriendo los métodos utilizados para esconder mensajes fue necesario diseñar nuevos métodos de esconderlos. Es así como surge la **criptografía**, una técnica en la cual en lugar de esconder la existencia del mensaje, se esconde su significado por medio de la encriptación. En este método al mensaje original, denominado **texto plano**, se le realiza una operación utilizando una clave, obteniendo así un nuevo mensaje conocido como **criptograma**, que sin la clave resulta incomprensible. Solo las partes involucradas son capaces de descifrar el texto plano utilizando la clave. Esto significa que ambas partes involucradas deben poder tener una clave en común que sea desconocida por el resto de las personas que podrían querer interceptar el mensaje para lograr una comunicación secreta.

Uno de los primeros dispositivos criptográficos diseñados fue la *escítala* espartana que se usaba en el año 500 A.C. El sistema consiste en enrollar una tira de cuero alrededor de la varilla sobre la cual se escribe el mensaje. Luego se desenrolla la tira quedando así letras sueltas escritas sobre la misma. Para descifrar el mensaje se debe volver a enrollar la tira sobre una varilla del mismo largo. Este tipo de sistema de encriptación se conoce como criptografía por transposición y se basa en reordenar la posición de las letras del mensaje. Por otro lado, existe la criptografía por sustitución en la cual se mantiene la posición de cada letra pero se cambia su identidad. Un ejemplo de esto es el cifrado César que constituye uno de los primeros usos de cifrado por sustitución que se conoce. Consiste en sustituir cada letra por otra letra, ubicada 3 lugares a la derecha en el abecedario. Al alfabeto paralelo por el que se sustituye cada letra se lo conoce como **alfabeto cifrado**. Para cada alfabeto original existen $\approx 4 \times 10^{26}$ formas de reordenarlo lo que hace imposible descifrar este tipo de cifrados mediante pruebas. Pero todo desarrollo de métodos de criptografía viene acompañado con avances en el **criptoanálisis**. Esto es, el estudio de métodos para decodificar un criptograma sin poseer la clave. Para descifrar los mensajes cifrados usando un alfabeto cifrado se desarrolló entonces un método de estudio de frecuencias, sacando ventaja de que hay letras que se repiten más que otras. Como solución a este problema se inventó un nuevo método de cifrado conocido como *Vigenère* que apareció en el siglo XVI en el cual se utilizaba múltiples alfabetos cifrados en simultáneo. A cada letra se le asociaba un alfabeto cifrado correspondiente con un corrimiento rígido distinto. Este método resultó más seguro ya que no era posible descifrarlo mediante el análisis de frecuencias. Recién en el siglo XIX se descubrió una forma de quebrarlo conocido como el método Kasiski que consistía en encontrar la longitud de la clave buscando secuencias de letras repetidas [2].

Al conocer el largo vuelve a resultar útil realizar un análisis de frecuencias.

Hoy en día, los métodos de criptografía mayormente utilizados son los **protocolos criptográficos de clave pública** [3] [4]. Estos protocolos son de tipo asimétrico: la clave utilizada para encriptar el mensaje es distinta a la utilizada para desencriptarlo. Este método fue propuesto por primera vez en 1976 por Whitfield Diffie y Martin Hellman. Se denominan como Alice y Bob a las partes que quieren intercambiar un mensaje secreto. En este tipo de métodos Bob primero elige una clave secreta que solo él conoce, y luego a partir de ella genera una clave pública que comparte con Alice. Alice entonces usa la clave pública para codificar su mensaje y enviarlo a Bob, quien la desencripta usando su clave privada. La seguridad de este método reside en que Bob no necesita compartir la clave privada y sin ella el mensaje es indescifrable. Al no ser compartida, la clave privada resulta aún mas difícil de descubrir. Una de las primeras implementaciones experimentales de este tipo de cifrado se conoce como RSA y fue desarrollado por Rivest, Shamir y Adleman en el Massachusetts Institute of Technology (MIT) en 1978 [5]. Para usar este protocolo, quien recibirá el mensaje elige dos números primos p y q y los multiplica obteniendo $n = p \times q$. Este número es parte de la clave pública y se utiliza para generar la clave privada. Ambas claves deben tener una relación para ser usadas para encriptar y desencriptar el mismo mensaje. La seguridad de este tipo de sistemas reside en que es fácil, en términos computacionales, multiplicar dos números primos, pero es difícil, computacionalmente hablando, factorizar un número n en dos números primos. Se denomina fácil a una operación rápida; cuyo tiempo de cómputo crece polinomialmente con el número de bits, y difícil cuando el tiempo de cómputo crece exponencialmente. La seguridad de internet, por ejemplo, es uno de los sistemas que depende, en parte, de este tipo de encriptación.

El problema con los sistemas de encriptación asimétrica es que su seguridad depende de los avances tecnológicos y teóricos y por ende pueden volverse obsoletos con el tiempo. Con respecto al protocolo RSA, en 1994 Peter Shor descubrió que con una computadora cuántica sería posible desarrollar un algoritmo rápido de factorizar un número en dos números primos [6]. Surgen así (o re-surgen, ya que eran conocidos desde tiempo anterior pero su uso no estaba justificado) otros tipos de sistemas de cifrado simétricos, en los cuales se usa la misma llave para encriptar y desencriptar el mensaje. Un ejemplo de estos métodos de cifrado es la **libreta de un sólo uso** (OTP por sus siglas en inglés, *One-Time-Pad*) descrito por primera vez en 1882 por F. Miller, para uso en sistemas telegráficos [7] y “re-inventado” y patentado en 1926 por G. Vernam [8]. En este tipo de esquemas se encripta el mensaje usando un sistema binario. La clave debe cumplir lo siguiente:

- Tener la misma cantidad de bits que el mensaje original
- Ser utilizada una única vez
- Debe ser aleatoria

Lo primero que se hace es pasar el mensaje de texto plano a código binario. Para ello primero se traduce el texto a un código de números usando el código ASCII, para luego pasar esa secuencia de números a código binario. Una vez generado el mensaje m_1 se genera una clave k del mismo largo. Realizando una suma de módulo 2 en binario (\oplus) se obtiene el criptograma $s = m_1 \oplus k$. Recordemos que al ser conmutativa esta suma, si se utiliza la misma clave dos veces entonces sería posible obtener el mensaje original sin poseer la clave usando los dos criptogramas: $s_1 \oplus s_2 = m_1 \oplus k \oplus m_2 \oplus k = m_1 \oplus m_2 \oplus k \oplus k = m_1 \oplus m_2$ donde se utilizó que $k \oplus k = 0$. En la figura 1.1 se muestra un ejemplo de como encriptar la palabra HOLA usando un protocolo de OTP.

| Letra | ASCII | Binario | | Texto plano | 01001000 01001111 01001100 01000001 |
|-------|-------|----------|---------------|-------------|-------------------------------------|
| H | 72 | 01001000 | \Rightarrow | Clave | 10011001 00110101 10001101 01100011 |
| O | 79 | 01001111 | | Criptograma | 11010001 01111010 11000001 00100010 |
| L | 76 | 01001100 | | | |
| A | 65 | 01000001 | | | |

Figura 1.1: Encriptación de la palabra “HOLA” usando el código de Vernam u OTP. Figura extraída de [9]

En la práctica, para encriptar un mensaje se usa un algoritmo asimétrico para generar una clave segura que luego se usa para implementar un algoritmo simétrico. Esto se hace porque los algoritmos asimétricos son muy lentos para utilizar sólo esos métodos. Como la seguridad de este tipo de sistemas no esta probada teóricamente, ya que los protocolos de encriptación asimétricos podrían llegar a ser vulnerables por nuevos desarrollos tecnológicos, la seguridad de estos sistemas está comprometida.

La **Distribución Cuántica de Claves** (QKD por sus siglas en inglés *Quantum Key Distribution*) surge como respuesta a este problema. QKD busca generar una clave segura de forma aleatoria entre dos estaciones. Para ello usa las propiedades de la mecánica cuántica por lo que su seguridad reside en propiedades fundamentales de sistemas cuánticos y no en capacidades tecnológicas del momento.

1.2 Fundamentos de la teoría de la información cuántica

1.2.1 Estados cuánticos, observables y evolución temporal

En la mecánica cuántica, los estados físicos están representados por vectores en el espacio de Hilbert (\mathcal{H}). En la notación de Dirac, los estados son representados por $|\psi\rangle$. Los espacios de Hilbert son espacios vectoriales complejos, con producto interno hermitiano y que satisfacen

el axioma de completitud. Si son finitos entonces pueden ser generados por una base ortonormal. Esto significa que cualquier estado puede, entonces, ser escrito como superposición de elementos de la base:

$$|\psi\rangle = \sum_a c_a |a\rangle, \text{ con } c_a \in \mathbb{C} \text{ tal que } \sum_a |c_a|^2 = 1 \quad (1.1)$$

Escrito de esta forma queda explícita una propiedad de la mecánica cuántica que no existe en la mecánica clásica: un sistema físico puede estar en múltiples estados en simultáneo.

Las propiedades observables del sistema se representan como operadores lineales \mathbf{O} que actúan sobre el espacio de Hilbert. Los posibles resultados de medir cada observable están dados por los autovalores o_n del mismo. A continuación se ejemplifica como aplicar un operador \mathbf{O} sobre el estado $|\psi\rangle$:

$$\mathbf{O}|\psi\rangle = \mathbf{O} \sum_a c_a |a\rangle = \sum_a c_a \mathbf{O}|a\rangle \quad (1.2)$$

Se observa que es posible actuar con un posible operador sobre varios estados a la vez. Esto permite procesar información en paralelo, reduciendo así el tiempo de cómputo.

La evolución temporal de los estados cuánticos en los espacios de Hilbert es descripta por operadores unitarios \mathbf{U} . Al ser unitario se cumple que el estado final $|\psi(t)\rangle = \mathbf{U}|\psi(0)\rangle$, es también un estado cuántico.

1.2.2 Mediciones

En la sección anterior se mencionaron cinco postulados de la mecánica cuántica. Existe un último postulado que dice que al medir un observable \mathbf{O} sobre el estado $|\psi\rangle$, la probabilidad de obtener el autovalor λ es $p_{\lambda_b} = \sum_{b/\lambda_b=\lambda} |\langle b|\psi\rangle|^2$ y que el estado luego de la medición $|\psi'\rangle$ está dado por la proyección del estado original sobre el subespacio asociado al autovalor λ medido:

$$|\psi'\rangle = \frac{1}{p_{\lambda}} \sum_{b/\lambda_b=\lambda} |b\rangle \langle b|\psi\rangle \quad (1.3)$$

Esto quiere decir que el estado se ve modificado por la medición. Esta es una propiedad fundamental de la mecánica cuántica y uno de los fundamentos que garantiza la seguridad de los protocolos de QKD.

1.2.3 Qubits y bases conjugadas

En la computación clásica la mínima unidad de información está dada por los bits, que pueden tomar un valor de 0 ó 1. Para la información cuántica existe un análogo denominado *qubit*. Un *qubit* es un estado cuántico que pertenece a un espacio de Hilbert de dimensión 2. Al ser un espacio finito se puede definir una base que tradicionalmente se representa como

$\mathcal{B} = \{|0\rangle, |1\rangle\}$. De esta forma, un estado genérico $|\phi\rangle$ puede escribirse como combinación lineal de los qubits; $|\phi\rangle = c_0|0\rangle + c_1|1\rangle$, con $|c_0|^2 + |c_1|^2 = 1$. Realizando una operación unitaria sobre esta base se obtienen otras bases válidas. Como se destacó más arriba, a diferencia de los bits clásicos, los *qubits* además de poder encontrarse en el estado $|0\rangle$ ó $|1\rangle$, se puede encontrar en una superposición de ellos.

Según el *principio de complementariedad*, si se prepara un objeto tal que la propiedad A toma un valor preciso, siempre existe otra propiedad B cuyo valor se encuentra completamente indeterminado. Dadas dichas condiciones se dice que las propiedades A y B son *complementarias* [10]. Esto significa que si se prepara el sistema en el que el resultado de medir la propiedad A está completamente determinado, al medir la propiedad B el resultado es completamente aleatorio. Las bases \mathcal{B}_A y \mathcal{B}_B definidas tal que los operadores complementarios **A** y **B** son diagonales en dichas bases, son complementarias y se denominan bases *conjugadas* ó *mutuamente no sesgadas*. Como se detallará más adelante, este tipo de bases son de especial interés en la criptografía cuántica. Para el caso de dimensión 2 existen tres operadores conocidos como los operadores de Pauli que definen bases mutuamente no sesgadas:

$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (1.4)$$

Tradicionalmente los autoestados de **Z** se denotan $\{|0\rangle$ y $|1\rangle\}$, los de **X** como $\{|+\rangle$ y $|-\rangle\}$ y los de **Y** como $\{|0_y\rangle$ y $|1_y\rangle\}$. Los autovalores asociados a estos estados son 1 y -1 respectivamente y todos estos pares de estados forman un espacio de Hilbert de dimensión 2. Es posible escribir los autoestados de **X** en función de los de **Z**:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (1.5)$$

Análogamente para los autoestados de **Y** se tiene que:

$$|0_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \quad |1_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \quad (1.6)$$

De la misma forma es posible también invertir estas relaciones y escribir los autoestados de **Z** en función de los de **X** ó **Y**. De esta forma, si se mide la propiedad **Z** sobre un qubit en el estado $|+\rangle$ hay una probabilidad $\frac{1}{2}$ de obtener 1 y de $\frac{1}{2}$ de obtener -1. Como son bases mutuamente no sesgadas, si se realiza una medición de dos operadores de Pauli distintos de manera consecutiva el resultado de la medición es completamente aleatorio.

1.2.4 Teorema de no clonación de estado cuánticos

Como se vio arriba, no es posible medir un sistema cuántico sin modificarlo. Esto agrega un nivel de seguridad a cualquier protocolo de codificación que utilice estados cuánticos, ya que un espía no puede medir el estado sin modificarlo y por ende, sin ser detectado. Sin embargo, si el

espía fuese capaz de clonar el estado sería capaz de pasar desapercibido y realizar mediciones sobre el estado clonado, y así obtener información del estado original sin modificarlo.

Para ver si esto es posible se supone que se tiene el estado $|\psi\rangle$ y se quiere realizar una copia del mismo. Para ello se necesita contar con otro estado, comúnmente denominado *ancilla*. Tomando, por ejemplo, el estado $|0\rangle$ como ancilla, el estado inicial conformado por ambos sistemas se puede escribir como $|\Psi\rangle_{AB} = |\psi\rangle \otimes |0\rangle$. A y B refieren a los sistemas. Si es posible clonar el estado, eso significa que existe un operador unitario U_{copy} que genera una copia del estado, es decir, evoluciona al estado de tal forma de obtener un estado final $|\Psi'_{AB}\rangle = |\psi\rangle_A \otimes |\psi\rangle_B$. El teorema de no clonación prohíbe la existencia de dicho operador: supongamos que existe U_{copy} y se lo utiliza para copiar dos estados $|\psi\rangle$ y $|\phi\rangle$:

$$\left. \begin{aligned} |\Phi'\rangle &= U_{copy}|\Phi\rangle = |\phi\rangle_A \otimes |\phi\rangle_B \\ |\Psi'\rangle &= U_{copy}|\Psi\rangle = |\psi\rangle_A \otimes |\psi\rangle_B \end{aligned} \right\} \xrightarrow{U_{copy}^{-1} U_{copy}=1} \langle\Phi'|\Psi'\rangle_{AB} = \langle\Phi|\Psi\rangle_{AB}$$

De dicha ecuación se obtiene que

$$\begin{aligned} \langle\Phi'|\Psi'\rangle &= \langle\Phi|\Psi\rangle \\ (\langle\phi|_A \otimes \langle\phi|_B) (|\psi\rangle_A \otimes |\psi\rangle_B) &= (\langle\phi|_A \otimes \langle 0|_B) (|\psi\rangle_A \otimes |0\rangle_B) \\ \langle\phi|\psi\rangle_A \otimes \langle\phi|\psi\rangle_B &= \langle\phi|\psi\rangle_A \otimes \langle 0|0\rangle_B \\ \langle\phi|\psi\rangle^2 &= \langle\phi|\psi\rangle \end{aligned} \tag{1.7}$$

Esta condición sólo se cumple para estados ortogonales; para que exista el operador U_{copy} debe valer para todo $|\psi\rangle$ y $|\phi\rangle$, es decir, el resultado obtenido es absurdo. Este absurdo proviene de suponer que existe el operador U_{copy} . Vemos entonces que no es posible clonar un estado. Esta es una de las premisas fundamentales para la seguridad del protocolo de Distribución Cuántica de Claves.

1.3 Distribución Cuántica de Claves

La *Distribución Cuántica de claves* (abreviado: QKD) surge como un método para generar una clave segura entre dos partes cuya seguridad no dependa de los avances tecnológicos del momento. La seguridad del protocolo se basa en que es imposible medir una propiedad de estado cuántico sin perturbarlo, por lo que si un espía intenta interceptar la clave, afectaría la medición sería detectado. El teorema de no-clonación además asegura que no sea posible obtener información sin perturbar, ya que tampoco es posible generar una copia del sistema y medir sobre dicho estado para no ser detectado. Combinado con el protocolo de encriptación *One-Time Pad*, QKD conforma un protocolo de codificación seguro.

Todos los protocolos de codificación QKD requieren de dos canales de comunicación entre las partes que pretenden compartir la clave. Un canal público autenticado; clásico, y un canal

cuántico privado seguro. Al ser autenticado, un hipotético espía, que se denominará como Eve, es capaz de ver lo que se envía por el canal público pero no modificarlo.

La primer implementación de un protocolo de QKD fue propuesta por Charles Bennett y Gilles Brassard en 1984 [11] y que se conoce como BB84.

1.3.1 Protocolo BB84

El protocolo BB84 fue la primer propuesta para implementar un protocolo QKD + *One-Time Pad* entre dos entidades que se denominaran Alice y Bob. Se utilizan qubits en bases mutuamente no sesgadas. Usando el grado de libertad de polarización de fotones individuales, se pueden utilizar la base computacional ($+$: $|H\rangle$, $|V\rangle$), y la base diagonal (\times : $|D\rangle$, $|A\rangle$). Se asocia el estado 1 al estado $|H\rangle$ y al $|D\rangle$, y el estado 0 a $|V\rangle$ y a $|A\rangle$. Análogamente, es posible implementar el protocolo en cualquier sistema cuántico de dos niveles.

En primer lugar Alice prepara, de manera aleatoria, la polarización del fotón en uno de los cuatro estados posibles. Para ello primero elige una base ($+$ ó \times) y un estado (0 ó 1) de forma aleatoria (esta aleatoriedad de su decisión no es simple de realizar. Las computadoras son sistemas determinísticos y, por ende sólo son capaces de generar secuencias algorítmicas pseudo-aleatorias. Para ello entonces se deben utilizar sistemas físicos realmente no determinísticos. Por ejemplo, es posible usar la generación de fotones únicos usando *beam-splitters*). El objetivo aquí es no introducir correlaciones indeseadas entre las detecciones. Luego de generar el fotón en el estado deseado, Alice se lo envía a Bob mediante el canal cuántico privado. Bob debe detectar ese “qubit viajero”: para ello elige (sin conocer la elección de Alice) en qué base medir ($+$ ó \times) y registra el resultado de la medición. En el caso que ambos elijan la misma base los estados estarán correlacionados, ya que si Alice prepara el fotón en el estado 1(0) entonces Bob obtendrá el estado 1(0) al realizar la medición. Sin embargo, si ambos midieron en distintas bases, al ser estas bases mutuamente no-sesgadas, la probabilidad de que Bob obtenga el estado 0 ó 1 es 50%, independientemente del estado preparado por Alice. Este procedimiento se repite y al conjunto de bits registrados se lo conoce como clave cruda.

Una vez generada la clave cruda, cuyo largo es acordado previamente por ambas partes, se comienza la siguiente etapa. Aquí Alice comparte con Bob, por medio del canal clásico, las bases que eligió para cada medición, **sin compartir el resultado de la medición; sin compartir ni el bit enviado, ni el resultado de la medición del mismo**. Bob luego le comparte a Alice por el mismo medio la ubicación (dentro de la serie de símbolos enviados) de los bits en las que eligieron medir en la misma base. Luego, ambos descartan los bits en los que eligieron medir en distintas bases. Conservan los casos en los que eligieron las mismas bases, donde el estado preparado por Alice y el medido por Bob deben coincidir. Los bits resultantes conforman la *clave final* ó *tamizada*. En la figura 1.2 se muestra un esquema de un ejemplo de implementación de este protocolo.

| | | | | | | | | |
|------------------|---|---|---|---|---|---|---|---|
| Bases de Alice | + | × | + | + | × | × | × | + |
| Bits de Alice | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| Envío de fotones | | | | | | | | |
| Bases de Bob | × | × | + | × | + | + | × | + |
| Bits de Bob | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| Coincidencias | ✓ | ✓ | | | | | ✓ | ✓ |
| Clave tamizada | 0 | 0 | | | | | 1 | 0 |

Figura 1.2: Ejemplo de implementación del protocolo BB84 para generar la clave de *bits* a partir de la clave cruda entre Alice y Bob, en la que intercambian 8 símbolos. Figura extraída de [9]. Alice prepara un fotón eligiendo una base (+ ó ×) y el estado. Luego lo envía por el canal cuántico a Bob, quien elige en que base medir el fotón recibido y guarda el resultado de la medición que puede valer 0 ó 1. Luego, ambos comparten a través del canal clásico las bases elegidas y guardan los bits obtenidos en los casos que las bases elegidas coinciden, obteniendo así la clave tamizada.

1.3.2 Ataques y su detección

Una vez generada la clave tamizada comienza la tercera etapa, en la cual se busca poder detectar un espía, si lo hubiese. Eve es un espía que desea descubrir la clave secreta que comparten Alice y Bob; para hacerlo deberá interceptar el canal cuántico, ya que la clave nunca es compartida por el canal público. Si Eve mide el fotón enviado por Alice y no lo reenvía a Bob, entonces Bob detectará la ausencia del fotón y no podrá asignar un estado (0 ó 1) a ese símbolo, por lo tanto no contribuirá a la clave. Entonces, Eve debe lograr detectar el fotón preparado por Alice, realizar una medición y luego reenviarlo a Bob. Este tipo de ataque se conoce como *intercept-resend*. Al momento de ejecutar esta acción de intromisión en el canal, medición y preparación, Eve desconoce las bases elegidas por Alice y por Bob, ya que esta información se revela *después* de la medición cuántica de Bob, por lo que Eve debe elegir bases de medición y preparación sin información respecto la base elegida por Alice. Cuando Bob y Alice compartan las bases usadas, los únicos símbolos relevantes corresponderán a los casos en que ambas bases coincidieron. Sobre esos casos, en la mitad de ellos Eve tendrá suerte y habrá elegido la misma base que Alice; en ese caso su acción no será detectada. Pero en la otra mitad de los casos utilizará una base incompatible con la que usaron Alice y Bob, modificando el estado. Como la elección de la base utilizada para generar el fotón es aleatoria, Eve no podrá predecir que base fue elegida y se equivocará el 50 % de las veces. Esto hace que luego del filtro de la clave cruda para generar la clave tamizada, si Eve actúa sobre todos los símbolos enviados por Alice, por un lado ella obtendrá un 50 % de la información de la clave y por otro lado un 25 % de las veces generará un error en la clave compartida por Alice y Bob.

Para detectar un ataque de tipo *intercept-resend*, Alice y Bob comparten, por medio del canal público, una parte de la clave final, que luego eliminan de la clave. En el ejemplo más simplificado de implementación de un protocolo de corrección de errores, Alice y Bob no

comparten los bits exactos sino que comparten el número XOR (suma en base 2) de dos bits elegidos. A partir de los valores de la clave compartida Alice y Bob calculan la Tasa de Error Cuántico (QBER por sus siglas en inglés *Quantum Bit Error Rate*), que corresponde al porcentaje de error entre las claves. El QBER se utiliza para determinar la seguridad de la clave ya que la presencia de un espía se ve reflejada en este valor. Dependiendo del valor de QBER obtenido conservan o descartan la clave. Cuanto más larga la parte de la clave compartida es menos probable que un espía no sea detectado. Luego de la corrección de errores realizan un proceso de *amplificación de privacidad* en la cual en lugar de utilizar la clave tamizada: Alice calcula el valor XOR sobre un par de bits y reemplaza los bits por el valor calculado. Le informa por medio del canal clásico a Bob la posición de los bits elegidos, quien hace lo mismo. De esta forma si un espía no fue detectado, luego de esta operación tiene menos información sobre la clave generada.

Si no hay fallas ni ineficiencias experimentales, todo lo que puede hacer Eve es la estrategia planteada arriba. La cantidad de clave segura extraíble de un protocolo funcionando en condiciones ideales es función de la tasa de error de transmisión. Sin embargo, los sistemas reales tienen fallas en la implementación inevitables. A los ataques que aprovechan estas fallas se los denomina en el ámbito de la criptografía ataques de canal lateral *side-channel attacks*. *Photon number splitting* (PNS) es un tipo de ataque que explota una de estas deficiencias de implementación: no existen fuentes determinísticas de fotones únicos. Entonces no es posible enviar fotones “únicos”, sino que se envían pulsos de luz tenues. Las fuentes de fotones usadas son las de pulsos coherentes atenuados, cuya estadística de fotones obedece a una distribución de Poisson (ver en la siguiente sección) por lo que, aún con flujos de fotones por pulso muy bajos, existe una probabilidad no nula de tener pulsos con más de un fotón. Esto le permitiría a Eve interceptar los fotones, conservar un fotón, enviar el resto y una vez publicadas las bases utilizadas medir sobre el fotón almacenado sin ser detectada. Como solución a este tipo de ataques entre 2003 y 2005 se desarrollaron los protocolos denominados de estado señuelo, en los cuales los pulsos ópticos que se envían tienen distintas intensidades: la operación de intercepción de un único fotón por parte de Eve produce una atenuación distinta para cada intensidad de pulsos enviados, y esto puede ser detectado [12] [13].

1.4 Implementación física de los qubits

Para la implementación de un protocolo de Distribución Cuántica de Claves se utilizan *qubits*. Como *qubit* es posible utilizar cualquier sistema de dos niveles. El método más utilizado en la actualidad para protocolos de comunicación cuántica es la codificación en algún grado de libertad físico de fotones únicos. Durante la transmisión de fotones a través del canal cuántico, los fotones deben ser protegidos de ruido ambiente, donde se considera ruido a una perturbación del grado de libertad de codificación del qubit. Se usan en la actualidad dos tipos de canales

para la comunicación cuántica con fotones: la fibra óptica y la propagación por aire. En este trabajo se utilizaron fibras ópticas monomodo para la banda C de telecomunicaciones (≈ 1550 nm) como canal cuántico.

1.4.1 Fuente de fotones

Para la implementación ideal de Distribución Cuántica de Claves se utilizan estados de Fock de un único fotón. Sin embargo, con las tecnologías actuales este tipo de estados resultan difíciles de generar [14]. En la práctica, se utilizan láseres atenuados ó pares de fotones entrelazados, donde el número de fotones (o de pares) generados sigue una distribución de Poisson. El problema con este tipo de estados es que hay una probabilidad no nula de generar múltiples fotones lo cual vuelve inseguro el protocolo.

En el primer caso se generan pulsos de luz con un láser y una serie de atenuadores que llevan la intensidad del haz a unos pocos fotones por pulso, generando un estado coherente con valor medio μ . Este es el tipo de fuente utilizada en este trabajo. La probabilidad de hallar n fotones este estado está dada por la siguiente ecuación:

$$P(n, \mu) = \frac{\mu^n}{n!} e^{-\mu} \quad (1.8)$$

Usando atenuadores es posible reducir μ indefinidamente, reduciendo así la probabilidad de que haya más de un fotón en un pulso no vacío, que es aproximadamente $\frac{\mu}{2}$ para $\mu \ll 1$. La desventaja es que reducir μ también aumenta el número de pulsos vacíos: $P(0, \mu) \approx 1 - \mu$ para $\mu \ll 1$. Para detectar estos estados de pocos fotones se utilizan detectores de conteo (en nuestro caso un módulo de conteo basado en un fotodiodo de avalancha). Estos detectores tienen cuentas de oscuridad, que son un error del instrumento y que ocurren cuando un detector indica que le llegó un fotón sin que eso ocurra. Al aumentar el número de pulsos vacíos se incrementa la proporción de cuentas de oscuridad con respecto fotones enviados, lo cual aumenta el error instrumental, y en el mejor de los casos, es decir aún si las cuentas de oscuridad fueran despreciables, la eficiencia del protocolo disminuye, ya que la cantidad de símbolos “vacíos”, es decir sin fotones que llevan información, es mucho mayor que la cantidad de símbolos con al menos un fotón. En la actualidad, la mayoría de las implementaciones de este tipo de fuentes usan $\mu \approx 0.1$, de forma que de los pulsos no vacíos, un 0.5% contienen más de un fotón.

Es preciso mencionar que dentro de los protocolos posibles de variable cuántica discreta, existe toda una familia de protocolos basados en estados entrelazados, el primero de ellos denominado E91 por su autor y el año de su invención (A. Eckert, 1991) [15]. La descripción y las tecnologías involucradas en esta clase de protocolos va más allá del objetivo de esta tesis. Una recopilación de los protocolos básicos y sus implementaciones se puede encontrar en la referencia [16].

1.4.2 Canal cuántico - fibras ópticas

Como canal cuántico en un protocolo QKD las dos opciones principales son las fibras ópticas ó la transmisión por aire. La elección del canal óptico depende de qué longitud de onda se utilizará para la comunicación, del largo del canal y del tipo de enlace. Se puede utilizar luz de 800 nm ó longitudes de onda en el rango de las telecomunicaciones (1300 nm ó 1550 nm). Las fibras ópticas del rango de telecomunicaciones tienen menor atenuación (0.35 dB/km para longitudes de onda de 1300 nm, y de 0.2 dB/km para 1550 nm) en comparación con las fibras especiales necesarias para la transmisión en 800 nm, donde la señal se atenúa 2 dB/km como se muestra en la figura 1.3. Con lo que respecta la detección y transmisión de los fotones, trabajar en el rango de 800 nm cuenta con la ventaja de que los detectores de fotones únicos en este rango (basados en silicio) tienden a ser más eficientes y menos ruidosos que los del infrarrojo cercano. Sin embargo, la inmensa mayoría de componentes optoelectrónicos (moduladores, conmutadores, multiplexores por longitud de onda, separadores de haz, polarizadores, etc) están optimizados para longitudes de onda entre los 1300 y 1550 nm. El problema es que no es posible utilizar las fibras ópticas ya implementadas por lo que requiere de nuevas instalaciones. Por otro lado, si se utilizan longitudes de onda entre 1300 nm ó 1550 nm, se pueden utilizar las fibras que se utilizan en telecomunicaciones pero es necesario desarrollar nuevos detectores. Esto se debe a que los detectores basados en semiconductores de silicón se vuelven transparentes para longitudes de onda por encima de los 1000 nm y por ende no pueden ser utilizados. Es por esto que, en general, se trabaja con longitudes de onda en el rango de telecomunicaciones ópticas. En el presente trabajo se utilizaron fuentes de luz, fibras ópticas, detectores y otros componentes optoelectrónicos específicos para la tercera ventana óptica de telecomunicaciones, centrada en 1550 nm.

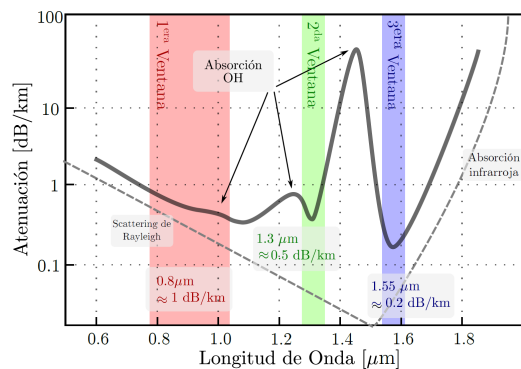


Figura 1.3: Atenuación de fibras monomodo en función de la longitud de onda utilizada. Las bandas de color representan las tres ventanas de comunicaciones: 800 nm, 1300 nm y 1550 nm. Figura extraída de [17].

Existen dos tipos de fibras: las fibras monomodo y las fibras multimodo. Las fibras multimodo tienen un núcleo más ancho, con un diámetro de alrededor de 50 μm , que permite guiar

múltiples modos en simultáneo. En estas fibras los modos se pueden acoplar por lo que no son una buena opción como canal cuántico ya que el acoplamiento genera ruido. Por otro lado, las fibras monomodo tienen un núcleo más angosto, el tamaño depende de la longitud de onda a propagar pero en general son de aproximadamente 10 μm . Este tipo de fibras resultan ser un canal adecuado para la comunicación cuántica entre Alice y Bob. Sin embargo, existen todavía problemas en su estabilidad. Imperfecciones en la fibra generan efectos como la birrefringencia, la dispersión por modo de polarización, las pérdidas dependientes de la polarización y los cambios en fase geométrica, que reducen la estabilidad de la luz propagada por la fibra.

La birrefringencia es la presencia de dos velocidades de fase distintas para dos estados de polarización ortogonales. Es causada por asimetrías en la fibra ó diferente tensión alrededor del núcleo de la misma. Existen un tipo de fibras conocidas como *polarization maintaining* (PM) que son diseñadas con alta birrefringencia tal que se acoplen los dos modos de polarización ortogonales. En los canales cuánticos se utilizan combinaciones lineales de modos ortogonales de polarización, que en este tipo de fibra fluctúan rápidamente, por lo que las fibras PM no son adecuadas como canales cuánticos. A su vez, la estabilidad de la birrefringencia requiere que las fluctuaciones térmicas y mecánicas sean lentas.

La polarización por modo de dispersión ocurre cuando la velocidad de grupo de polarizaciones ortogonales es distinta. También es causado por imperfecciones en la fibra. Produce que los pulsos se ensanchen en formas distintas por lo que pueden llegar a solaparse. Es un efecto estocástico y depende de la raíz del largo de la fibra utilizada. Es fácil de corregir cuando se usan fuentes de láseres tenues usando un láser con longitud de coherencia grande, pero para fuentes de pares de fotones resulta más complicado solucionarlo.

Las pérdidas dependientes de la polarización es la presencia de diferente atenuación en polarizaciones ortogonales. Sus efectos son insignificantes en la transmisión de la fibra pero afecta los componentes ópticos como los moduladores de fase.

Por otro lado, cambios en temperatura y en la tensión mecánica de la fibra producen cambios en el índice de refracción de la misma lo cual genera fluctuaciones en la fase de la luz. Al modificar el índice de refracción, la fase acumulada en cada camino tiene fluctuaciones en las escalas de las variaciones térmicas y mecánicas que se encuentran entre los Hz y kHz.

Por lo dicho, la polarización como grado de libertad cuántico para preparar, transmitir y detectar qubits en fibra no es el método más práctico, y como mínimo requiere de un sistema de estabilización activo de la polarización a lo largo de todo el canal. En la actualidad se realizan experimentos de Distribución Cuántica de Claves donde se emplea otro tipo de codificación en qubit que no se ve afectada por los efectos descritos anteriormente que afectan la polarización de la luz [18]. Para eludir estos efectos se utilizan *qubits* generados por pulsos ópticos codificados en modos temporales discretos de luz con una fase relativa entre ellos. La polarización sigue siendo inestable pero las fluctuaciones ya no son en el grado de libertad de codificación, que ahora es el tiempo, o mejor dicho la fase relativa entre dos pulsos ópticos

separados un tiempo mucho menor que los tiempos característicos de las fluctuaciones térmicas y/o mecánicas.

1.4.3 Modos temporales discretos de fotones: *time-bin*

Se mencionó en la sección anterior que codificar en polarización resulta en numerosos problemas en su implementación por ruido causado por efectos de birrefringencia, dispersión de modos de polarización, pérdidas dependientes de la polarización, entre otros. Como alternativa surge la codificación en el modo temporal discreto de los fotones o *time-bin*. La separación temporal entre los pulsos utilizados esta usualmente en el orden de los pocos nanosegundos, o incluso por debajo del nanosegundo; éstas son escalas temporales mucho menores que los tiempos característicos de fluctuaciones térmicas y mecánicas. De esta forma el sistema de codificación es insensible a la polarización reduciendo así el ruido. La codificación en *time-bin* aún requiere de interferómetros estables para la detección de los *qubits* pero utilizan fibras de menos de 10 m de longitud mientras que si se quiere codificar en polarización es necesario mantener estable una fibra de kilómetros de longitud.

En primer lugar es preciso definir la base computacional que se utilizará en *time-bin*. Cada símbolo está definido por dos modos temporales continuos separados por una distancia Δt como se muestra en la figura 1.4. Estos intervalos temporales pueden (ó no) estar ocupados por un pulso de luz coherente en cada uno, con un valor medio de fotones total por símbolo μ . Se define el primer estado de la base cuando se encuentra ocupado el primer modo temporal y vacío el segundo. Este estado se lo conoce como *early* y se nota $|e\rangle \equiv |0\rangle$. Análogamente, se define al segundo estado de la base; *late*: $|l\rangle \equiv |1\rangle$. Una vez definidos los estados de la base computacional es posible pasar a definir las bases mutuamente no sesgadas (MUBs) que se utilizaran en la codificación. Los estados se construyen superponiendo los estados de la base computacional $|e\rangle$ y $|l\rangle$ y modificando la fase relativa entre ambos pulsos. En la figura 1.4 se muestra cómo se definen los distintos estados de las bases diagonal y circular (en analogía con las bases no sesgadas de polarización), variando la fase para obtener los 4 estados con los que se trabajará luego.

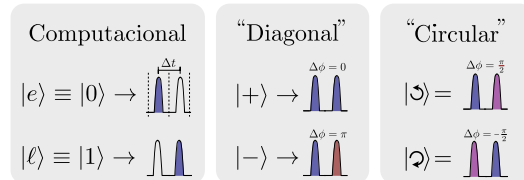


Figura 1.4: Bases de la codificación de *qubits* en el modo temporal discreto de los fotones. En primer lugar se define la base computacional en función al tiempo de llegada de los fotones. A partir de ello se definen dos bases mutuamente no sesgadas como superposición de los estados de la base con una fase relativa. Figura extraída de [19].

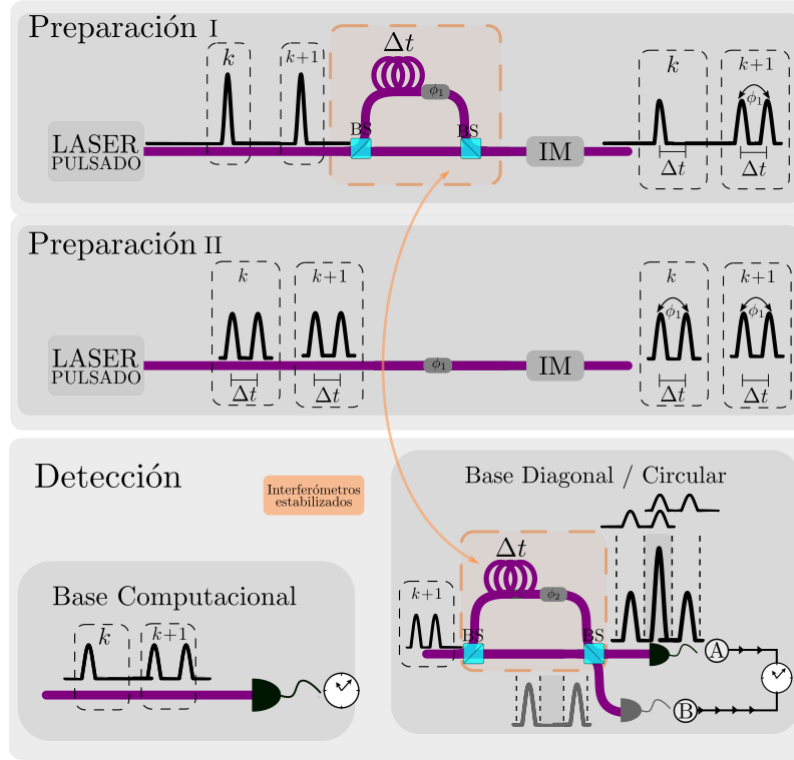


Figura 1.5: Esquema experimental para la preparación y detección de un estado *time-bin* donde el *qubit* se encuentra codificado en el modo temporal discreto de la luz y utilizando la fase relativa entre dos pulsos. Para ambas operaciones se utiliza un interferómetro con un desbalance de caminos Δt . Para la preparación de estados se presentan dos opciones: usando un interferómetro de Mach-Zehnder (preparación I) ó generando un par de pulsos con un láser pulsado (preparación II). En la preparación I se generan dos copias de un pulso de luz coherente usando un primer interferómetro y se controla la fase relativa ϕ_1 por medio de un modulador de fase. Por otro lado, en la preparación II se generan dos pulsos de luz con el láser y luego se introduce una fase ϕ_1 entre ellos usando un modulador de fase para obtener el par de pulsos con fase relativa. Para la detección se utiliza un segundo interferómetro con un modulador de fase que introduce una fase relativa ϕ_2 entre ambos caminos. Se producen tres modos temporales a la salida, donde el central es el que tiene la información de fase que define el estado. Figura extraída de [19]

En la figura 1.5 en el recuadro preparación I se muestra un método de preparar estados *time-bin* usando un láser pulsado, un interferómetro de Mach-Zehnder y un modulador de intensidad (IM). Cada pulso es dividido por el *beam-splitter* generando así dos copias del mismo a la salida del interferómetro donde uno de ellos tiene un retardo temporal Δt por haber viajado por el camino largo del interferómetro. Para seleccionar entre los estados de la base computacional se utiliza el modulador de intensidad. Para generar el estado $|e\rangle$ ($|l\rangle$) se obtura el segundo (primer) modo temporal. Se utiliza un modulador de fase en el camino largo del interferómetro para introducir una fase ϕ_1 en el pulso que viaja por el camino largo

del interferómetro. Los moduladores de fase introducen un desfase modificando el índice de refracción de la fibra por medio del efecto electro-óptico. Estos dispositivos introducen una diferencia en el camino óptico entre los brazos del interferómetro del orden de la longitud de onda (en los cientos de nanómetros) mucho menor al ancho del pulso (típicamente entre 0.5 y 1.0 ns, es decir que se extienden entre los 10 y 20 cm sobre una fibra de índice de refracción $n = 1.5$), por lo que no se modifica significativamente el camino óptico. A continuación se muestra el estado generado a partir de un solo pulso en la preparación:

$$|\psi\rangle = \alpha|e\rangle + \beta e^{i\phi_1}|\ell\rangle; \quad |\alpha|^2 + |\beta|^2 = 1. \quad (1.9)$$

Existen otros métodos alternativos para generación de estados *time-bin*. En el presente trabajo, por ejemplo, se generan dos pulsos de luz intensa usando una señal eléctrica que es enviada al láser. Luego se introduce con un modulador de fase una fase relativa entre los mismos y se atenúa la señal para obtener pulsos de luz de pocos fotones. Este sistema se muestra en la figura como preparación II. Este método evita tener que lidiar con las fluctuaciones de fase que podría incorporar el interferómetro de preparación. Además, al incorporar el modulador de fase al camino común de ambos pulsos (y no sólo en el camino largo), con suficiente resolución temporal es posible codificar más de un símbolo con el mismo modulador digital, según se aplique un cambio de fase al primero, al segundo, o a ambos pulsos.

Para detectar los estados *time-bin* es suficiente con registrar el tiempo de llegada de los fotones. Realizar proyecciones en las bases, sin embargo, resulta más complicado. Para ello es necesario utilizar un segundo interferómetro con desbalance de caminos. Usando un desbalance de caminos adecuado, tal que la diferencia de tiempo de transito entre los caminos es Δt , se obtienen tres estados a la salida del interferómetro. El efecto de pasar por el camino largo se puede expresar de la siguiente manera:

$$\begin{aligned} |e\rangle &\rightarrow |e + \Delta t\rangle = |\ell\rangle \\ |\ell\rangle &\rightarrow |\ell + \Delta t\rangle, \end{aligned} \quad (1.10)$$

Luego, si se hace pasar el estado preparado (ecuación 1.9) por el segundo interferómetro, a la salida A del mismo se obtiene el siguiente estado:

$$|\psi\rangle_A = \frac{i}{2} \{ \alpha|e\rangle + \beta e^{i\phi_1}|\ell\rangle + \alpha e^{i\phi_2}|e + \Delta t\rangle + \beta e^{i(\phi_1+\phi_2)}|\ell + \Delta t\rangle \}$$

De los tres *bins* que se obtienen a la salida de la detección, la información respecto el estado del *qubit* se encuentra en el *bin* del centro. Los estados en cada salida entonces se muestran resumidos a continuación, donde se escribió en gris la parte que no aporta información sobre el estado.

$$\begin{cases} |\psi\rangle_A = \frac{i}{2} \{ \alpha|e\rangle + (\beta e^{i\phi_1} + \alpha e^{i\phi_2})|\ell\rangle + \beta e^{i(\phi_1+\phi_2)}|\ell + \Delta t\rangle \} \\ |\psi\rangle_B = \frac{i}{2} \{ \alpha|e\rangle + (\beta e^{i\phi_1} - \alpha e^{i\phi_2})|\ell\rangle - \beta e^{i(\phi_1+\phi_2)}|\ell + \Delta t\rangle \} \end{cases} \quad (1.11)$$

A partir de los estados, y tomando como ejemplo el caso $|\alpha| = |\beta| = \frac{1}{\sqrt{2}}$ es posible obtener la probabilidad de detectar un fotón en el tiempo l en cada salida, del segundo interferómetro en función de la diferencia entre las fases ϕ_1 y ϕ_2 .

$$\begin{aligned} P_{(A,\ell)}(\psi) &= |\langle \ell | \psi \rangle_A|^2 = \frac{1}{2} \cos^2(\tilde{\phi}), \\ P_{(B,\ell)}(\psi) &= |\langle \ell | \psi \rangle_B|^2 = \frac{1}{2} \sin^2(\tilde{\phi}) \quad \text{y} \\ \tilde{\phi} &= \frac{\phi_1 - \phi_2}{2}. \end{aligned} \quad (1.12)$$

Se observa que la probabilidad de detectar un fotón en la salida A ó B del segundo interferómetro depende de la diferencia de fases. Usando estos resultados se puede realizar una tabla con las probabilidades de detección de un fotón en cada tiempo y en cada salida. La misma se muestra en la figura 1.6. Se observa que la probabilidad de detección en los tiempos e y $l + \Delta t$ son independientes de las fases y vale $\frac{1}{8}$ para ambas salidas: A y B. Por otro lado, la probabilidad de detectar un fotón en el tiempo $|\ell\rangle$ en cada detector depende de las fases elegidas.

| | Proy. Base Diagonal | | | | Proy. Base Circular | | | |
|-------------------------------|---------------------|-----------------------|-------------|------------------------|---------------------|-----------------------|-------------|------------------------|
| ϕ_2 | 0 | | | | $\frac{\pi}{2}$ | | | |
| ϕ_1 | $0_{(D)}$ | $\frac{\pi}{2}_{(Q)}$ | $\pi_{(A)}$ | $\frac{3}{2}\pi_{(Q)}$ | $0_{(D)}$ | $\frac{\pi}{2}_{(Q)}$ | $\pi_{(A)}$ | $\frac{3}{2}\pi_{(Q)}$ |
| $P_{(B,\ell)}(\psi)$ | 1/2 | 1/4 | 0 | 1/4 | 1/4 | 0 | 1/4 | 1/2 |
| $P_{(A,\ell)}(\psi)$ | 0 | 1/4 | 1/2 | 1/4 | 1/4 | 1/2 | 1/4 | 0 |
| $P_{(X,e)}(\psi)$ | 1/8 | 1/8 | 1/8 | 1/8 | 1/8 | 1/8 | 1/8 | 1/8 |
| $P_{(X,\ell+\Delta t)}(\psi)$ | 1/8 | 1/8 | 1/8 | 1/8 | 1/8 | 1/8 | 1/8 | 1/8 |

Figura 1.6: Probabilidad de detección en cada tiempo en las distintas salidas del interferómetro. Las fases ϕ_1 y ϕ_2 son las fases introducidas por los moduladores de fase del primer y segundo interferómetro respectivamente. En los tiempos de llegada e y $l + \Delta t$ la probabilidad es independiente del estado. En los casos que la probabilidad es igual para cada salida A ó B, se denota la salida con la letra X. De la probabilidad de detección en el bin temporal “ l ” es posible obtener información sobre el estado preparado. Figura extraída de [19].

Se demostró que la probabilidad de detección de un fotón, o lo que es equivalente, la intensidad a la salida del interferómetro utilizado en la detección, en el tiempo l depende de la fase relativa. Haciendo la analogía con la codificación en polarización, la elección de base y estado por parte de Alice consiste en elegir la fase ϕ_1 utilizada para preparar el estado *time-bin*. $\phi_1 = \{0, \pi\}$ corresponden a la base diagonal y $\phi_1 = \{\frac{\pi}{2}, \frac{3\pi}{2}\}$ a la base circular. El *bit* 0 esta

asociado a $\phi_1 = \{0, \frac{\pi}{2}\}$, y el *bit* 1 a $\phi_1 = \{\pi, \frac{3\pi}{2}\}$. Por otro lado, en la detección Bob elige en que base medir eligiendo $\phi_2 = \{0, \frac{\pi}{2}\}$. Si la diferencia de fase $\phi_2 - \phi_1 \in \{0, \pi\}$ entonces las bases elegidas son compatibles y los valores de bit asociado al estado preparado por Alice y detectado por Bob son los mismos. Si, por lo contrario, $\phi_2 - \phi_1 \in \{\frac{\phi}{2}, \frac{3\pi}{2}\}$, las bases son incompatibles y los resultados deben ser descartados. Esto se muestra ejemplificado en la tabla a continuación.

| Alice | | Bob | | |
|---------------|----------|----------|-------------------|---------------|
| Valor del bit | ϕ_1 | ϕ_2 | $\phi_1 - \phi_2$ | Valor del bit |
| 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | $\pi/2$ | $3\pi/2$ | ? |
| 1 | π | 0 | π | 1 |
| 1 | π | $\pi/2$ | $\pi/2$ | ? |
| 0 | $\pi/2$ | 0 | $\pi/2$ | ? |
| 0 | $\pi/2$ | $\pi/2$ | 0 | 0 |
| 1 | $3\pi/2$ | 0 | $3\pi/2$ | ? |
| 1 | $3\pi/2$ | $\pi/2$ | π | 1 |

Tabla I: Tabla ejemplificando las posibles elecciones de ϕ_1 y ϕ_2 por Alice y Bob y los resultados obtenidos por cada uno. Si la fase relativa cumple que $\phi_2 - \phi_1 \in \{0, \pi\}$, los bits coinciden ya que se eligieron bases compatibles. Si $\phi_2 - \phi_1 \in \{\frac{\phi}{2}, \frac{3\pi}{2}\}$ el bit del estado detectado por Bob coincide con el preparado por Alice solo el 50 % de las veces y debe ser descartado de la clave. Tabla extraída de [3]

Este tipo de sistemas de codificación en modos temporales discretos de la luz fue implementado experimentalmente con una fibra de 50 km de longitud por por Marcikic y Gisin en 2004 [18].

1.4.4 Detección

Otra parte crucial para la implementación de un protocolo de codificación de *qubits* en fotones son los detectores de fotones únicos. Existen en la actualidad múltiples candidatos entre los cuales están los fotomultiplicadores, los fotodiodos de avalancha, las junturas de Josephson superconductoras, entre otros instrumentos. Los fotodiodos de avalancha (APD por sus siglas en inglés *avalanche photodiodes*) son los más comúnmente utilizados. Los APD están compuestos por diodos semiconductores basados en junturas p-n. Hay tres semiconductores de utilidad: de silicio; que se utiliza para longitudes de onda debajo de $1 \mu m$, de Germanio, que pueden ser utilizados para longitudes de onda alrededor de $1.3 \mu m$, y los semiconductores de arseniuro de galio e indio (InGaAs) que pueden ser utilizados en ambas longitudes de onda de telecomunicaciones: $\lambda = 1.3 \mu m$ y $\lambda = 1.55 \mu m$.

El funcionamiento de este tipo de detectores opera en lo que se conoce como modo *Geiger*. En este modo la interacción entre el fotón y el semiconductor produce energía que supera la energía del *gap* entre las bandas de la juntura produciendo pares de electrón-hueco que producen avalanchas de electrones, produciendo así una corriente. En otras palabras, se induce un campo eléctrico que genera una diferencia de potencial que supera la tensión de ruptura del material produciendo una corriente de forma abrupta. La corriente producida indica la detección de un fotón. El tiempo de generación de la corriente está en el orden de los picosegundos. Luego de la generación de la avalancha de electrones se debe cortar la producción mediante un proceso conocido como *quenching*. Luego de la detección se disminuye la tensión de polarización del diodo por debajo de la tensión de ruptura. De esta forma se corta el proceso de ionización. Luego se vuelve a subir la tensión para preparar al detector para una nueva detección. Este proceso toma tiempo, por lo que genera un tiempo muerto (*dead-time* en inglés) entre las mediciones.

El proceso de detección usando el modo *Geiger* tiene dos fuentes principales de ruido. Por un lado, se encuentran las cuentas de oscuridad, que ocurren cuando se induce una avalancha de electrones sin que llegue un fotón al detector. Esto puede ocurrir, por ejemplo, por fluctuaciones térmicas, y el número de cuentas de oscuridad incrementa si se agranda la ventana de detección. Para reducir las cuentas de oscuridad se mantienen a los detectores en temperaturas bajas, alrededor de -20°C . Por otro lado están las fuentes de ruido conocidas como *afterpulses*, que son avalanchas que aparecen justo luego de una detección. Cuando se genera una avalancha por la detección de un fotón, aparecen portadores en niveles de energía intermedios que luego pueden inducir una segunda avalancha sin la llegada de un fotón. Este tipo de ruido puede ser reducido aumentando el tiempo muerto entre detecciones, a costa de reducir la frecuencia de detección.

En el presente trabajo se utilizó un detector IdQ-201 de IDQuantique de InGaAs/InP para detectar fotones con longitudes de onda de 1550 nm. Las ventanas de detección de este detector están entre los 2 ns y 100 ns. Se utiliza un reloj externo sincronizado a la llegada de fotones para definir el comienzo de una medición.

1.5 Otras aplicaciones de las fibras ópticas

En el presente trabajo se utilizaron fibras ópticas como canal cuántico para enviar información. Sin embargo, las fibras tienen otras aplicaciones, entre ellas, tienen un gran potencial como material de sensado. Las fibras ópticas son guías de ondas dieléctricas cilíndricas. El núcleo y revestimiento de las fibras esta hecho de vidrio ó plástico y esta recubierto por material acrilato o poliimida para protegerlo. Una de las propiedades interesantes de la fibra óptica es que son electromagnéticamente pasivas lo cual las convierte en buenos sensores. A su vez, uno de sus componentes principales es la sílice (dióxido de silicio), que resulta ser un material

resistente a la mayoría de los agentes químicos y biológicos, lo cual los hace de especial interés ya que pueden ser utilizados en materiales y ambientes en los que otros sensores no son de utilidad. También tienen baja atenuación óptica, por lo que pueden ser utilizadas para realizar mediciones a lo largo de grandes distancias, son capaces de resistir altas temperaturas y también pueden ser livianas y pequeñas, por lo que son más accesibles y fáciles de transportar. Todas estas propiedades convierten a las fibras ópticas en buenos sensores. Las fibras son de doble uso; por un lado pueden ser utilizadas para medir parámetros por medio de cambios en las propiedades de la luz que es propagada por la fibra y, a su vez, pueden ser utilizadas como medios de comunicación [20].

Los sensores de fibra óptica pueden ser clasificados de acuerdo a distintas propiedades. En primer lugar es posible clasificarlas según su ubicación en intrínsecas o extrínsecas. Un sensor de fibra óptica intrínseco es aquel en el que la fibra actúa como material de sensado y como medio de transporte de información. Este tipo de sensores es capaz de sensar sobre grandes distancias. Algunos ejemplos de este tipo de sensores son: sensado de temperatura usando dispersión de Raman en la fibra o pérdidas en la fibra dependientes de la temperatura; sensado de voltaje eléctrico mediante el análisis de la dependencia de la polarización con el voltaje o campo eléctrico aplicado; y el uso de la fibra óptica como hidrófono para el sensado sísmico. Por otro lado, los sensores extrínsecos son aquellos donde la fibra actúa como guía de la señal hacia y desde un sensor óptico. En estos casos la fibra actúa como medio de comunicación. Este tipo de sensores permite acceder a lugares que otros sensores no pueden como, por ejemplo, el motor de una aeronave. Un ejemplo de este tipo de sensores son los interferómetros de Fabry-Perót donde se usa una cavidad al final de la fibra como objeto de sensado.

En segundo lugar es posible clasificar los sensores de fibra óptica de acuerdo a su modo de operación [20]. Se pueden entonces clasificar los sensores en las siguientes categorías: sensores de modulación de intensidad, los cuales detectan cambios físicos y perturbaciones en la luz recibida pero son susceptibles a la potencia, por lo que requieren un sistema de referencia; sensores de modulación de longitud de onda que miden cambios en la longitud de onda de la luz que se propaga por la fibra; sensores de modulación de fase que explotan el principio de interferencia de la luz para medir propiedades de interés; sensores basados en un reflectómetro óptico en el dominio del tiempo (OTDR por sus siglas en inglés) los cuales detectan cambios en la luz dispersa en la fibra. Finalmente, existen los sensores basados en polarización que detectan cambios en la luz producidos por cambio en la polarización. Este tipo de fibras explotan el fenómeno de la birrefringencia. En esta tesis se trabajó con un interferómetro de Mach-Zehnder, que forma parte de los sensores de fibra por modulación de la fase junto con los interferómetros de Fabry-Perot, Michelson y Sagnac. Este tipo de sensores poseen alta sensibilidad y exactitud pero a un mayor costo.

En la cotidianidad, sin embargo, los sensores suelen ser separados en tres categorías princi-

pales: sensores de fibra basados en redes, sensores interferométricos y sensores por distribución. Los sensores ópticos basados en redes de Bragg en fibra son sensores en los cuales la información está codificada en la longitud de onda, lo cual permite que la señal sea fácilmente multiplexada. Se expone el núcleo de las fibras a un patrón de luz UV alterando así permanentemente el índice de refracción del núcleo. De esta forma la fase de la luz que viaja por la fibra varía. La longitud de onda reflejada resulta altamente sensible a la extensión de la fibra y cambios en la temperatura convirtiendo a este tipo de fibras en buenos sensores de tensión y temperatura. La longitud de onda de bragg (λ_B) depende linealmente con el índice efectivo de refracción (n_{eff}) y el periodo de la rendija (Λ): $\lambda_B = 2n_{eff}\Lambda$. La respuesta habitual de este tipo de fibras es de cambios de 0.64, 1 y 1.3 pm/ $\mu\epsilon$ ($\mu\epsilon$ = micro tensión) para longitudes de onda de 830, 1300 y 1550 nm respectivamente.

Parte del trabajo presentado aquí consiste en mitigar los cambios de fase impuestos en la diferencia de caminos de un interferómetro e inducidos por cambios en la temperatura o vibraciones mecánicas; los sensores interferométricos de fibra aprovechan esta sensibilidad para detectar mínimas variaciones de estos parámetros. Dentro de los más comunes se encuentran los interferómetros de Mach-Zehnder, Fabry-Perot, Michelson y Sagnac. El principio de funcionamiento para detectar, por ejemplo, sonido es que las ondas acústicas producen cambios de presión. Las fluctuaciones en la presión del aire tensiona la fibra lo cual modifica el índice de refracción de la fibra. Esto produce una variación en la fase de la luz propagándose a través de la fibra. En el caso de los interferómetros de Mach-Zehnder, se mide la fase relativa entre los caminos del interferómetro. Este tipo de sensores interferométricos se usa en la industria de telecomunicaciones, para sensado bajo el agua como hidrófono, para sensado de temperatura e índice de refracción y también en la medicina para realizar imágenes optoacústicas y para sensar la frecuencia cardíaca y respiratoria.

Finalmente, están los sensores distribuidos dentro de los cuales se sitúan los OTDR. Estos sensores estudian la luz dispersada dentro de la fibra. La fibra contiene dispersión por Rayleigh, Brillouin y Raman. La longitud de onda principal de la luz se llama componente Rayleigh, pero también hay longitudes de onda por encima y por debajo de ellas que contienen información sobre las propiedades locales de la fibra como la tensión y la temperatura. Son estas componentes las que se utilizan para sensar distintas propiedades de interés.

1.5.1 Monitoreo de signos vitales usando sensores de fibras ópticas

Con la mejora de calidad de vida, ha ido aumentando la atención de las personas con respecto a su salud. Cada vez más personas invierten en estudios para prevención y cuidado de su salud. Dentro de los parámetros a estudiar está la frecuencia cardíaca (HR por sus siglas en inglés *heart rate*) y frecuencia respiratoria (RR por sus siglas en inglés *respiratory rate*) que están directamente relacionadas a enfermedades asociadas a la edad como lo son la

enfermedad pulmonar obstructiva crónica (EPOC) e insuficiencia cardíaca congestiva. Por el momento los instrumentos tradicionales para medir HR y RR no resultan prácticos para el uso diario. Es en parte por ello que aparecen los sensores de fibra óptica, que son más livianos y fáciles de utilizar. Son, por ejemplo, más fáciles de integrar a un almohadón, lo que facilita su uso diario [21]. Una aplicación de este tipo de sensores es en el estudio de la respiración. La apnea de sueño, por ejemplo, es un trastorno común y potencialmente fatal del sueño que afecta 4 % de los hombres y 2 % de las mujeres a nivel mundial. Para estudiarlo se realizan estudios de RR; expresado en número de respiraciones por minuto y de *tidal volume*, que es la cantidad de aire que ingresa y sale de los pulmones en cada respiración, y aporta información sobre la profundidad de la respiración. Debido a que son estudios de sueño es necesario realizar estudios poco invasivos para alterar el sueño lo mínimo posible. Al usar fibras ópticas como material de sensado es posible estudiar el sueño del paciente de una manera menos invasiva, por lo que son de especial interés en este área de estudio.

Los sensores de fibra óptica interferométrica también se utilizan en aplicaciones relacionadas con la salud. Por ejemplo, uno de los brazos del interferómetro se usa como referencia y se mantiene aislado de cambios externos mientras que el otro brazo es el de sensado y se expone a perturbaciones externas que modifican la longitud y el índice de refracción de la fibra. De esta forma midiendo la variación de la fase relativa entre los caminos es posible extraer información respecto los parámetros a monitorear. En 2017 Li propuso el uso de un sensor basado en un interferómetro de Mach-Zehnder, en el cual el brazo de sensado se coloca dentro de la máscara de oxígeno y la fibra detecta cuándo hay cambios en la potencia óptica causados por deformaciones de la máscara durante la inhalación y exhalación [22]. Esto permite distinguir entre distintas condiciones de respiración. Este es un ejemplo de una de las posibles aplicaciones de un sensor de fibra óptica interferométrico como instrumento de estudio del sueño.

Otra aplicación interesante de este tipo de sensores es el estudio de la temperatura corporal. La temperatura corporal normal se encuentra entre 36.1 °C y 37.2 °C, si sube por encima de los 38°C se considera fiebre. La fiebre es evidencia de una infección o enfermedad por lo que resulta útil poder tener una medida de la temperatura corporal. En 2017 Cao presentó un sensor biocompatible de alto rendimiento basado en una cavidad Fabry-Perot llena con etanol [23]. Las franjas de interferencia producidas en la cavidad varían linealmente con la temperatura. De esta forma es posible diseñar un sensor con una sensibilidad de 0.429 nm/°C. Un año más tarde Wang propuso otro tipo de sensado de fibra óptica más fácil de construir usando un interferómetro de Mach-Zehnder [24]. Logró aumentar la sensibilidad a 8.962 nm/°C. En dicho trabajo se compararon los resultados de medición con el sensor de fibra óptica con la temperatura medida con un termómetro y se encontró que los resultados eran compatibles.

En resumen, el uso de fibras ópticas como instrumento de sensado tiene múltiples aplicaciones y resultan ser una buena alternativa más liviana y práctica. En esta sección se presentó un resumen de las distintas formas de explotar las propiedades de las fibras para utilizarlas

como sensores y también se ejemplificaron algunas de sus aplicaciones. Resulta entonces de gran interés conocer y poder caracterizar el uso de estas fibras y también de interferómetros de Mach-Zehnder en fibra, que además de ser utilizados en experimentos de criptografía cuántica, como en el presente trabajo, tienen gran potencial como material de sensado.

Capítulo 2

Interferometría de fuentes independientes

En este capítulo se describe el trabajo realizado para caracterizar la estabilidad en frecuencia de la fuente de luz que posteriormente se usará para caracterizar el interferómetro: esto es fundamental para poder determinar si la inestabilidad del interferómetro corresponde a inestabilidades del mismo, o si se debe a fluctuaciones en la longitud de onda de emisión de la fuente de luz.

2.1 Varianza de Allan

La varianza de Allan [25] surge como un método de caracterización de la estabilidad de sistemas oscilatorios. Es una medida de las fluctuaciones en frecuencia, permite distinguir entre distintos tipos de ruido y por ende se puede definir un tiempo óptimo de medición, a partir del cual los procesos de deriva dominan sobre las fluctuaciones estadísticas [26].

Se considera un oscilador de frecuencia característica ν_0 cuya fase $\Phi(t)$ tiene una dependencia temporal como se muestra en la siguiente ecuación:

$$V(t) = V_0 \text{ sen}(\Phi(t)), \quad \Phi(t) = 2\pi\nu_0 t + \phi(t) \quad (2.1)$$

Para este tipo de sistemas es posible definir la frecuencia instantánea $\nu(t)$ mediante la ecuación 2.2, y a partir de ella se define la frecuencia fraccionaria $y(t)$ como la desviación relativa de la frecuencia con respecto a ν_0 2.3.

$$\nu(t) = \frac{1}{2\pi} \frac{d\Phi(t)}{dt} = \nu_0 + \frac{1}{2\pi} \frac{d\phi}{dt} \quad (2.2)$$

$$y(t) = \frac{\nu(t) - \nu_0}{\nu_0} = \frac{1}{2\pi\nu_0} \frac{d\phi}{dt} \quad (2.3)$$

Luego se toman muestras \bar{y}_n que se definen como el promedio de la frecuencia fraccionaria \bar{y}_n en un intervalo temporal τ :

$$\bar{y}_n = \frac{1}{\tau} \int_{t_n}^{t_n+\tau} y(t) dt \quad (2.4)$$

La varianza de Allan se calcula como la esperanza de la diferencia cuadrática de valores consecutivos del valor medio de la frecuencia fraccionaria y queda determinada por la expresión

$$\sigma_y^2(\tau) = \frac{\langle (\bar{y}_{n+1} - \bar{y}_n)^2 \rangle}{2} \quad (2.5)$$

A partir de la varianza de Allan se define la desviación de Allan $\sigma_y(\tau)$ como la raíz cuadrada de la varianza.

$$\sigma_y(\tau) = \sqrt{\sigma_y^2(\tau)} \quad (2.6)$$

Dada una muestra de M valores de frecuencias es posible estimar la varianza de Allan $\sigma_y^2(t)$ a partir de los datos usando la ecuación 2.7.

$$\sigma_y^2(\tau) \approx \frac{1}{2(M-1)} \sum_{n=1}^{N-1} (\bar{y}_{n+1} - \bar{y}_n)^2 \quad (2.7)$$

Hasta ahora se detalló cómo calcular la varianza de Allan a partir de mediciones en frecuencia pero también existe una definición de la varianza que permite calcularla a partir de las fluctuaciones en fase. La ecuación se muestra en la fórmula 2.8. Se define $x(t)$ como la variable de tiempo fraccionario y se la puede calcular integrando las frecuencias fraccionarias.

$$x(t) = \frac{\phi(t)}{2\pi\nu_0}, \quad y(t) = \frac{dx(t)}{dt} \quad (2.8)$$

De esta forma la varianza de Allan se puede estimar a partir de $x(t)$ de la siguiente forma:

$$\sigma_y^2(\tau) \approx \frac{1}{2(N-2)\tau^2} \sum_{n=1}^{N-1} (x_{n+2} - 2x_{n+1} + x_n)^2 \quad (2.9)$$

Existe también otro tipo de varianza de Allan llamada varianza de Allan con superposición [27] donde se toman muestras que se superponen entre sí. El beneficio de usar esta varianza sobre la descrita anteriormente es que se reduce la variabilidad de los resultados de la varianza. Definiendo τ_0 como el tiempo de medición y m como el factor de promedio tal que $\tau = m\tau_0$ se puede estimar la varianza de Allan con superposición en función de la frecuencia o en función de la fase.

$$\sigma_y^2(\tau) \approx \frac{1}{2m^2(M-2m+1)} \sum_{j=1}^{M-2m+1} \left(\sum_{i=j}^{j+m-1} (\bar{y}_{i+1} - \bar{y}_i) \right)^2 \quad (2.10)$$

$$\sigma_y^2(\tau) \approx \frac{1}{2(N-2m)\tau^2} \sum_{n=1}^{N-2m} (x_{i+2} - 2x_{i+1} + x_i)^2 \quad (2.11)$$

En el presente trabajo se usó la desviación de Allan calculada a partir de la varianza de Allan con superposición de la frecuencia de batido entre dos láseres similares, para estudiar la estabilidad de la frecuencia de emisión del láser. Se buscó comparar la varianza de los datos con la varianza que se espera si solo hay ruido blanco, y se identificó la máxima precisión alcanzable para la diferencia de frecuencias de emisión de ambos láseres.

2.2 Láseres ITLA

Uno de los objetivos del presente trabajo fue estabilizar un interferómetro. Cuando se estudian las variaciones del interferómetro también hay que tener en cuenta las fluctuaciones de la fuente. Si, por ejemplo, la fuente es inestable para tiempos mayores a t_0 , entendiendo por estable un sistema cuyas fluctuaciones son menores a las fluctuaciones de ruido blanco, entonces no será posible conseguir que la condición de interferencia se mantenga estable por tiempos mayores a ese tiempo t_0 . Se caracterizó el funcionamiento y la estabilidad de los láseres y se estudiaron las fluctuaciones de su frecuencia.

2.2.1 Principio de funcionamiento

Como fuentes de luz para la caracterización del interferómetro se usaron módulos integrales láser sintonizables (Integrable Tunable Laser Assembly, ITLA) modelo PPCL550 de Pure Photonics [28]. En la figura 2.1a se muestra una foto de este láser. La cavidad esta formada por un chip de ganancia o medio activo de InP, en conjunto con una cavidad externa con un espejo de salida de alta reflectividad, como se muestra en la figura 2.1b. Dentro de la cavidad hay una serie de filtros etalon de silicio cuyos rangos espectrales libres difieren ligeramente. De esta forma, la curva de transmisión de los filtros selecciona, mediante el efecto Vernier [29], el pico del láser dominante. Este tipo de armado permite controlar independientemente la frecuencia, variando la temperatura de los filtros, y la potencia, la cual se modifica variando la corriente enviada al chip de ganancia. El sistema permite variar la frecuencia entre 191.5 THz y 196.5 THz con una resolución de 100 MHz, y la sintonía fina habilita cambiar la frecuencia con una resolución de 1 MHz. A su vez es posible controlar la potencia hasta 13.5 dBm (22 mW).

La electrónica de control también está integrada dentro del producto. La salida de potencia está regulada mediante un fotodiodo y la temperatura de los filtros es controlada mediante sensores de temperatura. A su vez, la estabilidad de la frecuencia de emisión se controla imponiendo una señal *dither* de 888Hz. Incluido en el dispositivo hay un micro-procesador que permite controlar el láser mediante una interfaz gráfica en una PC.

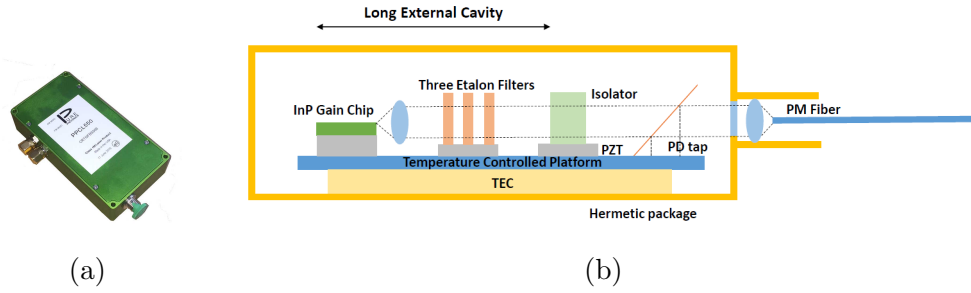


Figura 2.1: Figuras del láser sintonizable ITLA de Pure Photonics. En la figura (a) se muestra una foto del modelo usado en los experimentos mientras que en la figura de la derecha (b) se muestra un esquema del armado del láser. Ambas figuras fueron extraídas de la página del fabricante [30]

2.2.2 Modos de uso

Lo primero que se hizo fue estudiar el funcionamiento del láser. El mismo tiene dos modos de operación: modo “*whisper*” y modo “*dither*” [31]. En el modo *dither* los lazos de control están en funcionamiento, generando ruido en el rango 1 - 10 000 Hz. En este modo se fija la frecuencia seleccionada controlando la temperatura de los filtros de etalon y se impone una modulación de muy baja amplitud de aproximadamente 800 Hz para fijar la frecuencia a un máximo de transmisión de alguno de los etalon. Por otro lado, en el modo *whisper* se deshabilitan la máxima cantidad posible de lazos de control, reduciendo así el ruido en el rango debajo de los 10 000 Hz. Durante usos prolongados de este modo se debe volver a habilitar el modo *dither* cada cierto tiempo para asegurar que el láser esté en la frecuencia de emisión deseada.

2.2.3 Caracterización de estabilidad.

Una vez caracterizados los modos de funcionamiento, se buscó estudiar la estabilidad del láser. Esto se hizo en dos etapas: primero se hizo una medición de la frecuencia absoluta, en el rango de los GHz. Para ello se midió de forma directa con un Analizador de Espectros Ópticos (O.S.A. por su sigla en inglés) Burleigh WA1000, que dispone de un estándar de referencia de frecuencia interno (pero cuya resolución está limitada a los 100 MHz). El analizador de espectros óptico Burleigh tiene una exactitud (y resolución) de ± 1 ppm. Es decir, que puede medir la frecuencia de emisión del láser de la banda C de telecomunicaciones de 1550 nm (~ 193 THz) con una resolución de 0.001 nm (~ 100 MHz) [32]. Posteriormente se midió la precisión de la frecuencia de emisión, con una medición de relativa comparando la frecuencia de dos láseres similares. Para la primera parte se utilizó el montaje experimental de la figura 2.2. Se usó el analizador de espectros óptico para leer la diferencia en frecuencia (Δf) con respecto a la frecuencia arbitraria fijada externamente, en este caso de 193 THz. Para leer los

datos del O.S.A. de forma automatizada se usó un osciloscopio digital siglent SDS 1102CML.

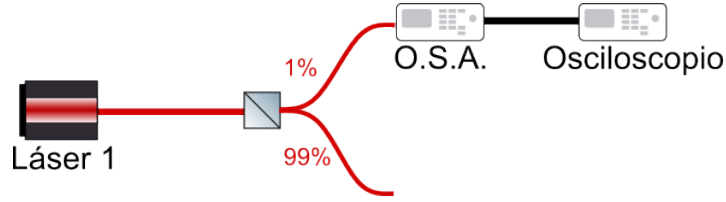


Figura 2.2: Esquema experimental para el estudio de la estabilidad en frecuencia del láser ITLA. Se usa un *splitter* para separar la luz de salida del láser y enviar el 1% de la luz al analizador de espectros O.S.A.. Para poder extraer los datos medidos por el O.S.A. se lo conectó a un osciloscopio del cual se toman los datos desde la PC.

El O.S.A. es un instrumento de la década de 1990; no posee una salida digital de los datos procesados; lee los datos de $\Delta f = f - f_0$ con $f_0 = 193$ THz en este caso (el valor de referencia f_0 se selecciona del panel frontal del equipo), y entrega una señal analógica proporcional, consiste en un voltaje que varía entre -10 V y +10 V, que registramos con un osciloscopio. Debido a esto fue necesario realizar una calibración para pasar de voltaje medido por el osciloscopio a Δf del analizador de espectros óptico. Para ello se fijó la frecuencia del láser nominalmente en 193.5 THz y se hizo un barrido fino entre 193.49 THz y 193.51 THz en pasos de 1 GHz. Esto se hizo mediante la interfaz con una conexión USB entre el láser y la PC. Con estos datos y las lecturas de voltaje se calibró la salida analógica del analizador de espectros. En la figura 2.3 se muestran los datos medidos junto con el ajuste de estos datos. El voltaje de salida depende linealmente con la frecuencia registrada por el O.S.A. Se obtuvo la función de correlación: $\Delta f(V) = (-25,308 \pm 0,093) \frac{GHz}{V} \times V + (-1,029 \pm 0,022) GHz$.

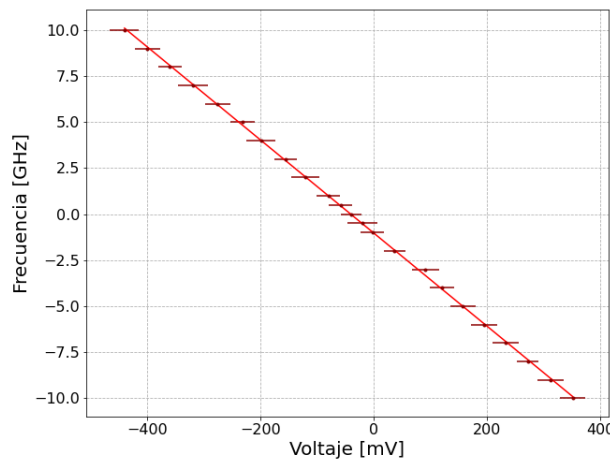


Figura 2.3: Calibración para pasar de voltaje entregado por el O.S.A. a diferencia de frecuencia del láser ITLA. $\Delta f(V) = (-25,308 \pm 0,093) \frac{GHz}{V} \times V + (-1,029 \pm 0,022) GHz$.

Antes de medir la salida del láser se caracterizó el ruido propio del sistema de registro y detección. Para ello se levantó la señal enviada por el analizador de espectros óptico al osciloscopio durante 100 minutos con el láser apagado. En la figura 2.4a se puede ver que hay una deriva de la señal en tiempos característicos de algunos minutos. En la figura de la derecha (figura 2.4b) se muestra, en azul, la desviación de Allan de la medición y en violeta la desviación de Allan si sólo hubiese ruido blanco.

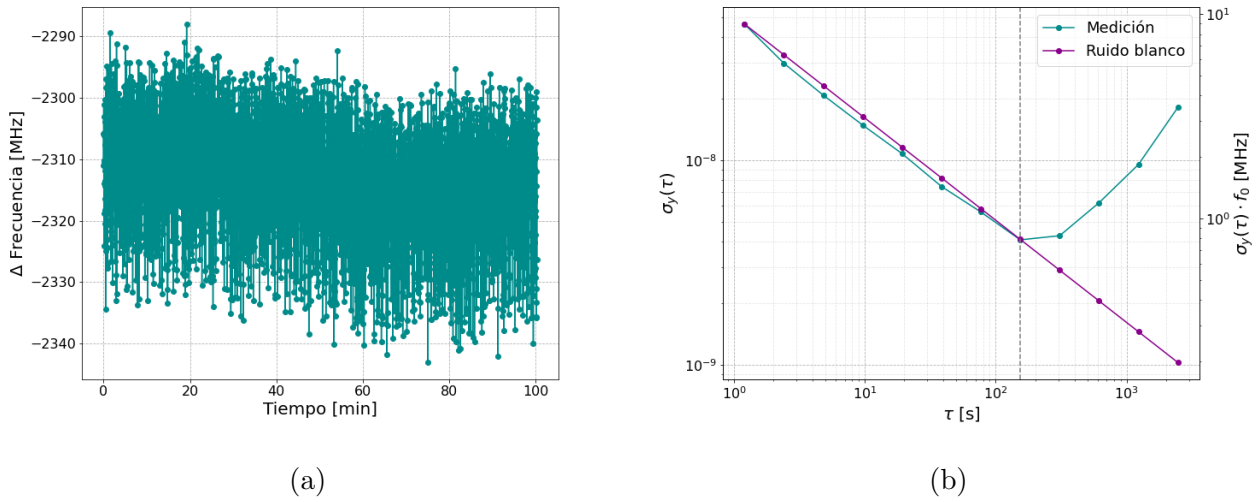


Figura 2.4: Mediciones de ruido del sistema de medición con el láser apagado. (a) Variación en frecuencia con láser apagado. En promedio la señal de salida toma un valor de (-2312.9 ± 9.0) MHz. (b) Desviación de Allan de medición de ruido. Hasta los 150 s la medición y el ruido blanco tienen pendientes similares y luego difieren indicando que hay otras fuentes de inexactitud.

Se observa que para tiempos menores a 150 s ambas varianzas tienen tendencias similares y luego la de la medición comienza a crecer en lugar de decrecer. Esto, junto con la deriva de la medición, sugieren la presencia de otros ruidos además del ruido blanco cuyos efectos se vuelven significativos luego de 150 s y que limita nuestro tiempo máximo de medición a tiempos menores a 150 s. Para tiempos de observación de este orden, el ruido del sistema puede acotarse a un equivalente en diferencia de frecuencias de centenas de kHz.

Con las caracterizaciones anteriores, podemos estudiar cómo fluctúa la frecuencia de emisión del láser durante el encendido. En la figura 2.5 se puede ver que tiene una variación significativa al inicio y luego de medio minutos la frecuencia ya se encuentra más estable por lo que es prudente esperar 1 minuto entre el encendido del láser y la toma de mediciones.

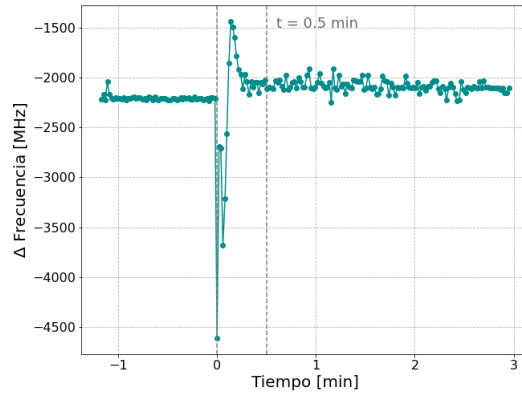


Figura 2.5: Variación de la frecuencia de emisión del láser (programada en $f=193.5$ THz) respecto a la frecuencia de referencia $f_0 = 193$ THz seleccionada en el O.S.A. Se define el inicio del tiempo como el momento en el que se encendió el láser. Se observa que la frecuencia tiene un salto y fluctúa significativamente hasta estabilizarse luego de medio minuto.

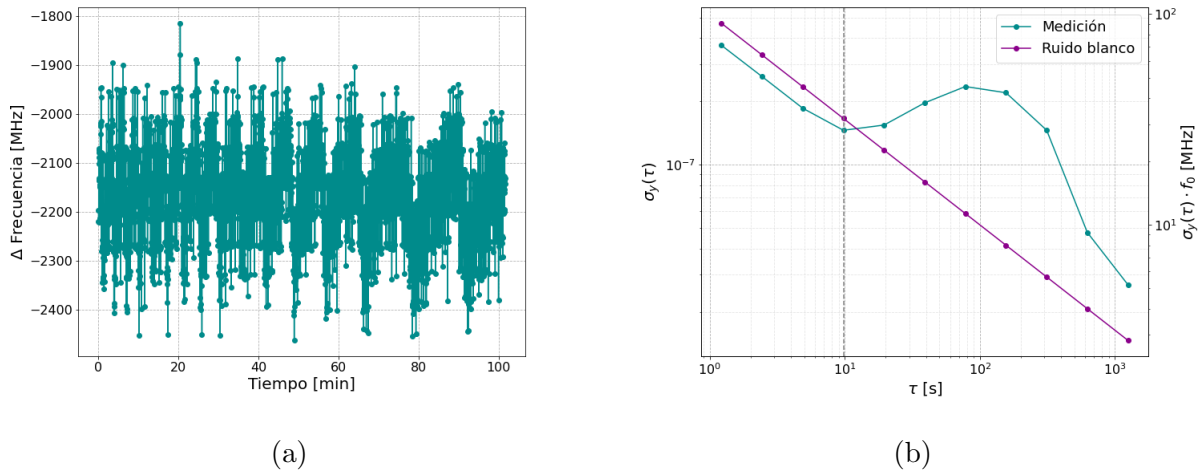


Figura 2.6: Mediciones de estabilidad de la frecuencia del láser con el mismo en modo *whisper*. (a) Variación en frecuencia del láser; la frecuencia de emisión se fija a una diferencia de 2200 MHz respecto una referencia arbitraria del O.S.A. (b) Desviación de Allan de medición de estabilización. Hasta los 10 segundos el ruido predominante es el ruido blanco.

Una vez caracterizado el método de medición se midió la estabilidad de la frecuencia del láser. Los resultados directos de la medición del analizador de espectros ópticos se muestran en la figura 2.6. Se observa que la frecuencia realiza un proceso cíclico que se va ralentizando con el tiempo, lo que sugiere algún tipo de termalización. En la figura 2.6b se graficó la varianza de allan de la medición con el láser encendido en modo *whisper*. Aquí se observa que la desviación de los datos tiene pendiente similar a la desviación de ruido blanco únicamente hasta los 10 segundos. Uno podría asumir que esto indica que el sistema es estable por 10

segundos. Sin embargo, durante ese tiempo hay menos de 10 mediciones realizadas por lo que no es suficiente para asegurarse que el sistema estuvo estable. Como se verá más adelante, el láser tiene fluctuaciones en el orden de decenas de MHz que es un orden menor que la resolución del instrumento y por ende no se pueden sacar conclusiones definitivas acerca de la estabilidad en este armado experimental: el límite de resolución del O.S.A. es 1 pm, esto es mayor que las fluctuaciones máximas de la frecuencia de emisión del láser estudiado.

Por este motivo, para caracterizar las fluctuaciones del láser, es necesario usar otro método que, aunque pueda no ser tan exacto como un espectrómetro calibrado, tenga más precisión para resolver la magnitud de esas fluctuaciones. El método elegido es generar interferencia entre dos sistemas láser equivalentes y estudiar las fluctuaciones del par.

2.3 Medición de estabilidad a partir de los batidos de dos láseres

Para comparar la estabilidad de la frecuencia de salida del láser en los distintos modos de funcionamiento se estudió la frecuencia moduladora de los batidos entre 2 láseres ITLA con una frecuencia de 193THz. Idealmente, se compara el dispositivo a estudiar con un sistema de referencia (un patrón de frecuencias, un láser amarrado a una referencia espectroscópica, etc). Como aún no se dispone en el país de un dispositivo de ese tipo en el rango de frecuencias de telecomunicaciones lo que se hizo fue comparar dos sistemas similares. Como no nos interesa estudiar la exactitud del valor de la frecuencia de emisión sino que nos enfocamos en su precisión, este método permite obtener una medida de las fluctuaciones de la diferencia de frecuencias de emisión del par de emisores.

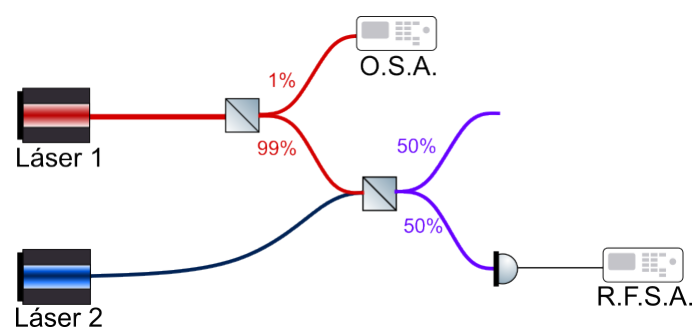


Figura 2.7: Esquema experimental para el estudio de batidos entre dos láseres ITLA con frecuencias de 193 THz y diferencia de frecuencias en los cientos de megahertzios. La salida de uno de los láseres se separa con un *tap* ó *splitter* desbalanceado. El 1 % de la señal se usa para monitorear la frecuencia mediante el O.S.A. La otra salida (de 99 %) se mezcla con la salida del segundo láser mediante un *splitter* 50:50 produciendo así batidos que son detectados y procesados con un fotodiodo Thorlabs DET08CFC/M (5GHz de ancho de banda) y el analizador de espectros de RF.

Para esta caracterización se usó el armado experimental que se muestra en la figura 2.7. En el esquema, usamos el O.S.A. para medir la frecuencia de uno de los láseres. El R.F.S.A, en cambio, es un analizador de espectros en el rango de radiofrecuencias (RF) Rigol DSA815 que fue utilizado para medir la frecuencia de batidos entre los láseres. Como se verá a continuación, las fluctuaciones de frecuencia están por debajo del límite de resolución de este instrumento. Con respecto al analizador de espectros RF, el mismo tiene un rango de frecuencias entre 9 kHz y 1.5 GHz y una resolución de hasta 1 Hz [33].

En las figuras a continuación se muestra el espectro de frecuencias de batido entre los dos láseres ITLA habiendo fijado una diferencia de frecuencias de 500GHz entre ellos. En los gráficos se observa que en el modo *dither* aparecen múltiples frecuencias producidas por los lazos de control de este modo mientras que en el modo *whisper* la frecuencia está mejor definida. Si bien deshabilitar los lazos es una ventaja cuando se necesita, durante otras mediciones se observó que después de varias horas encendido el láser en modo *whisper* aparecen ruidos y era necesario volver al modo *dither* y luego volver al modo *whisper* para quitarlos. Como los tiempos de medición requeridos fueron menores a 2 horas, tiempo en el cual el modo *whisper* funciona correctamente y tiene menor ruido que el modo *dither*, se procedió a trabajar con el láser en modo *whisper*.

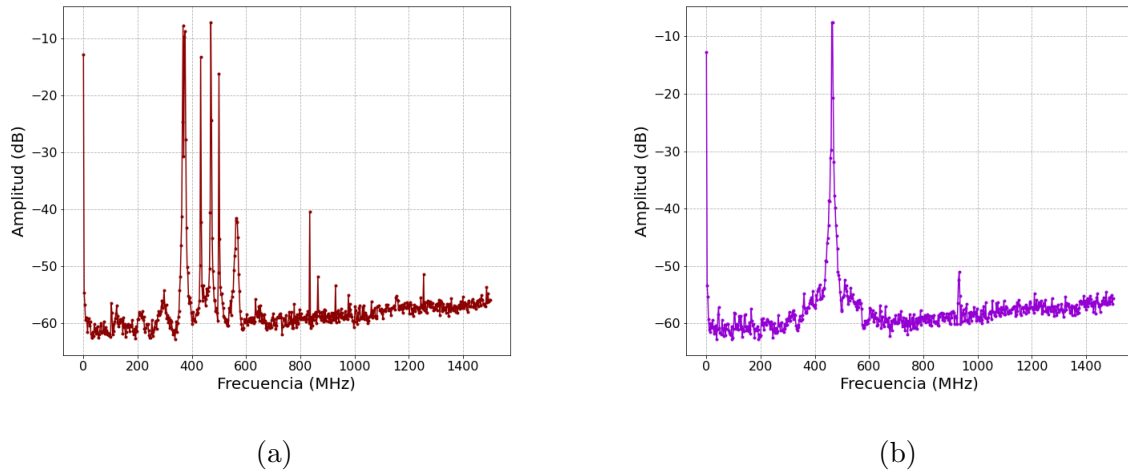


Figura 2.8: Frecuencia moduladora de batidos de dos láseres ITLA con frecuencias en el rango de los terahercios y diferencia de 500 MHz. (a) Modo de funcionamiento *dither*. Se observan varias frecuencias. En este modo están habilitados los lazos de control que producen ruido. (b) Modo de funcionamiento *whisper*. Se observa que la frecuencia es más estable que en el modo *dither*.

2.3.1 Interferencia de dos fuentes de luz independientes

En esta subsección se presenta otro método de caracterización de fluctuaciones en la frecuencia del láser, que, si bien no da una medida absoluta de las mismas, permite ver las

fluctuaciones relativas entre dos láseres similares pero independientes, con mucha mayor precisión que la alcanzable con el O.S.A. El mismo consistió en hacer interferir dos láseres ITLA, uno de ellos el estudiado en la sección anterior y un segundo láser idéntico. Se fijaron las frecuencias de ambos láseres en 193 THz. La interferencia entre ambos campos se da en un separador de haces acoplado a fibra óptica. De las mediciones se observa que hay una diferencia en los cientos de megahercios entre las frecuencias de los láseres. El beneficio de estudiar los batidos en lugar de la frecuencia del láser es que al ser una frecuencia de 4 órdenes de magnitud menor las fluctuaciones son mas notorias. Además, como esta frecuencia se encuentra en los cientos de MHz, se usó el analizador de espectros en radiofrecuencias para detectar la señal. El armado experimental es equivalente al de la sección del análisis de modos que se muestra en la figura 2.7.

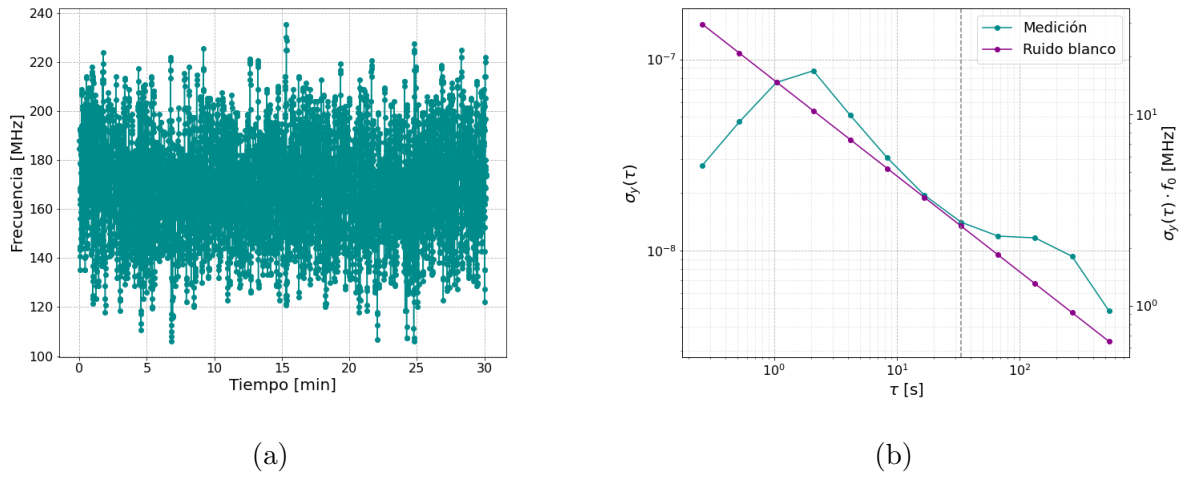


Figura 2.9: Mediciones de estabilidad de la frecuencia del batido entre láseres. (a) Variación en frecuencia de la frecuencia de batidos. La frecuencia en promedio toma un valor de (168 ± 20) MHz. (b) Desviación de Allan de medición de batidos. La varianza crece en los primeros 4 datos producto de un filtro pasa-bajos y luego empieza a tener comportamiento análogo al de ruido blanco hasta los 30 s.

En la figura 2.9a se muestra la frecuencia de batido entre los láseres. Para ambos láseres puestos a funcionar a una frecuencia nominal de 193 THz, el batido tiene, en promedio, un valor de (168 ± 20) MHz. Se observa que es un orden de magnitud menor que las mediciones de variación de frecuencia obtenida con el O.S.A. a partir de un único láser. Esto es una posible indicación de que dicho instrumento está trabajando en el límite de su resolución, y los efectos observados en la sección anterior es un fenómeno artificial generado por el propio sistema de detección y no en el dispositivo estudiado. Con respecto la desviación de Allan se observa que, a diferencia de las mediciones anteriores, la misma crece para los 4 primeros datos en lugar de decrecer. Este comportamiento puede explicarse si, por ejemplo hay un filtro pasa-bajos, o un mecanismo de integración a la entrada del analizador de espectros de RF,

en cuyo caso para tiempos de observación cortos hay una disminución de las fluctuaciones provocada por este filtrado, causando así una pendiente positiva en el gráfico de la desviación de Allan. La pendiente de la varianza tiene pendiente similar a la del ruido blanco hasta los 30 s de medición. Esto indica que hay un ruido o una deriva en los datos que afectan las mediciones luego de medio minuto. De todas maneras, para tiempos de observación más largos las fluctuaciones siguen disminuyendo, pudiéndose alcanzar exactitudes por debajo de los 5 MHz. Es razonable concluir que para futuros experimentos mientras las mediciones duren menos de 30 s el láser es considerado lo suficientemente estable, y en ese intervalo temporal es posible realizar promedios de los datos medidos.

Capítulo 3

Interferometría de una única fuente en dispositivos de fibra óptica

En este capítulo se detalla el trabajo realizado para estudiar la estabilidad de un interferómetro de Mach-Zehnder balanceado (los dos brazos de igual longitud) y desbalanceado. Se buscó estabilizar el mismo en temperatura, para lo cual primero se diseñó un gabinete contenedor de aluminio para aislarlo del entorno y luego se diseñó, construyó y caracterizó un control de temperatura para estabilizar la temperatura. Para estas caracterizaciones se usó uno de los láseres descriptor en el capítulo anterior.

3.1 Montaje experimental interferómetro de Mach - Zehnder

Para implementar experimentalmente un protocolo de Distribución Cuántica de Claves (Quantum Key Distribution, QKD) es necesario usar interferómetros estables donde sea posible controlar la fase entre ambas ramas. Es por esto que parte del objetivo de este trabajo se centró en estabilizar un interferómetro de Mach-Zehnder como el que se muestra esquematizado en la figura 3.1 que luego se utilizó para experimentos de QKD. Como fuente de luz se usó el láser ITLA de Pure Photonics estudiado en la sección anterior de 1550 nm. En el armado del interferómetro se usó fibra óptica monomodo normalizada ITU-T G.652D para el rango 1310/1550 nm [34]. Para dividir la luz en la entrada del interferómetro, y también para mezclarla en la salida, se usaron *splitters* 50-50 para fibra: acopladores ópticos de ventana dual (1310/1550 nm) de Thorlabs 10202A-50-FC [35]. Las conexiones entre acopladores y fibras se realizaron mediante acopladores de fibra FC/PC. En uno de los brazos del interferómetro se colocó un controlador de polarización manual del tipo “*bat ear*”, con el cual fue posible modificar el estado de polarización de la luz que atraviesa ese brazo. Esto permite maximizar el contraste del interferómetro, al igualar los estados de polarización sobre el *splitter* de salida. De esta

forma es posible compensar variaciones en la polarización de la fibra causadas, por ejemplo, por perturbaciones mecánicas. Cambiando el largo de alguno de los brazos del interferómetro es posible cambiar la configuración del interferómetro entre un interferómetro balanceado en el que ambos caminos tienen el mismo largo y un interferómetro desbalanceado en el cual uno de los caminos es más largo que el otro. Uno de los brazos del interferómetro incluye al *fiber stretcher* con sus cables de entrada y salida. Para compensar el retardo impuesto por este componente en el otro camino, la condición de balance de caminos se obtiene para un cable de fibra de largo aproximado $L_1 \approx 50$ cm. Respecto de la condición de interferómetro desbalanceado nuestro objetivo es generar un retardo entre caminos de aproximadamente 2 ns (que es la diferencia temporal adecuada para los pulsos de los símbolos de *time bin*). Este desbalance se obtuvo con un cable (*patchcord*) de longitud $L_2 = 110$ cm. En esta condición la diferencia de caminos ópticos entre ambos brazos del interferómetro es de $\Delta L = 2 \text{ ns} \times \frac{c}{n} \approx 40$ cm, donde c es la velocidad de la luz en vacío y n el índice de refracción del medio. Para una fibra SMF28 el índice de refracción es $n = 1.4682$. Este es el desbalance que se usará posteriormente como separación temporal entre los pulsos cuando se realicen con los experimentos de codificación en *time bin* con luz tenue.

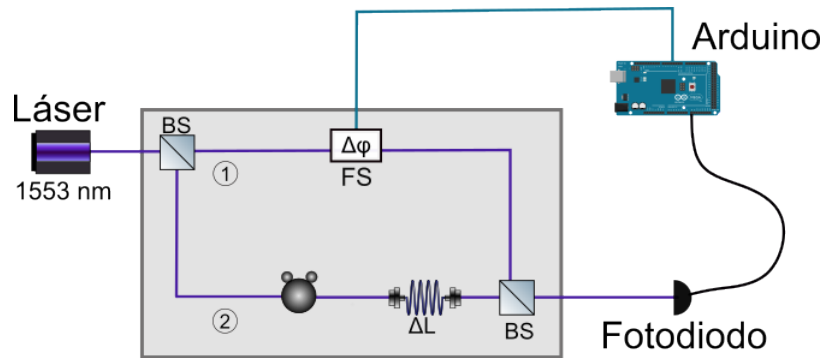


Figura 3.1: Esquema experimental del interferómetro de Mach-Zehnder a estabilizar. Se usa un *fiber stretcher* para introducir un desfase entre ambos caminos. Se cambia el largo ΔL de la fibra que está en el camino 2 para cambiar entre un interferómetro balanceado y desbalanceado.

En el otro camino del interferómetro se colocó un IDIL *fiber stretcher* [36] que permitió controlar el desfase entre los caminos. El *fiber stretcher* consiste en un arrollamiento de fibra alrededor de un material piezo-eléctrico. Este componente estira o acorta la fibra cuando se le aplica un voltaje. En el gráfico 3.2 se muestra la relación entre la elongación del material y el voltaje aplicado al mismo. Tiene una elongación máxima de 20 μm cuando se le aplica una corriente de 150 V. En este experimento se le aplicó una diferencia de voltaje de hasta 30 V, lo cual genera a una diferencia de camino equivalente a poco más de 3 longitudes de onda.

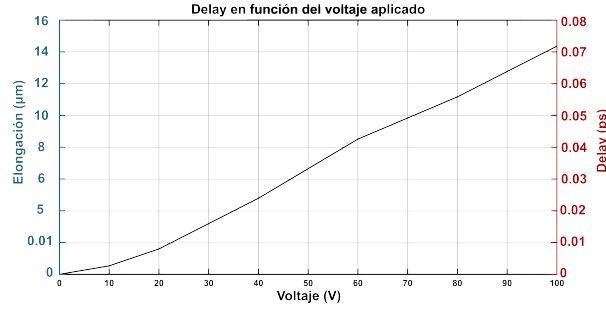


Figura 3.2: Elongación efectiva del camino óptico producida por el *fiber stretcher* en función del voltaje aplicado al mismo. Imagen extraída de [36]. Genera un estiramiento máximo de 20 μm al aplicarle un voltaje de 150V.

Para controlar el *stretcher* se usó un microcontrolador Arduino Mega 2560 [37]. El Arduino es una computadora integrada a una plaqueta. El mismo cuenta con 4 puertos serie UART y 16 entradas analógicas de 10-bit. Los pines de entrada analógica tienen resistencias de carga interna programable de 20-50 $\text{k}\Omega$ y pueden recibir una corriente máxima de hasta 40 mA. A su vez, pueden entregar una corriente máxima de 50 mA. Tiene un chip de interface USB UART (FTDI FT232RL) integrado en la plaqueta que permite comunicación con la PC mediante un puerto serie virtual. La PC también actúa como fuente para la plaqueta. El Arduino cuenta con un gestor de arranque (bootloader) que permite subir un nuevo código sin necesidad de un programador externo y que se comunica mediante un protocolo STK500. Del lado de la PC, se programa la placa mediante Arduino Software (IDE). Un inconveniente es que estas placas solo pueden generar voltajes entre 0V y 5V. Es por esto que a la salida de la placa se utilizó un convertor digital-analógico (DAC) MCP4921 de 12 bit de resolución con interface SPI controlado por medio de la placa, lo cual permite transformar el rango 0V - 5V a un rango -15V - 15V. Dicho circuito se encuentra esquematizado en la figura 3.3.

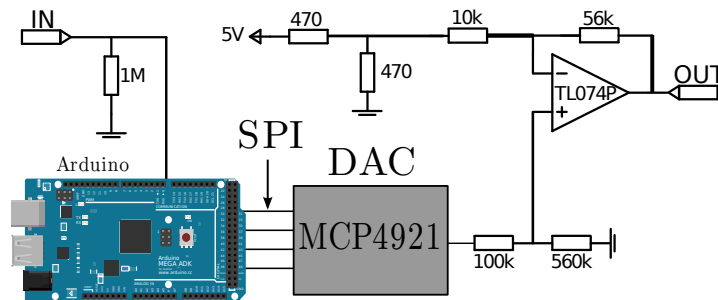


Figura 3.3: Esquema del circuito que permite convertir el rango de la salida de Arduino de 0-5V a -15 - 15V. Imagen extraída de [17]

Para estabilizar la temperatura del interferómetro se construyó también un gabinete contenedor diseñado a medida. El mismo está compuesto por placas de aluminio soldadas, de 4mm de espesor y fue fabricado por el Departamento de Prototipos de CITEDEF. Las dimensiones del gabinete son 14 cm x 10 cm x 8 cm. Se buscó minimizar el volumen de la caja lo cual faci-

lita controlar la temperatura del mismo. Se estudió el comportamiento de la fase con la tapa puesta o sin la tapa. En la figura 3.4 se muestra una foto del gabinete contenedor construido.

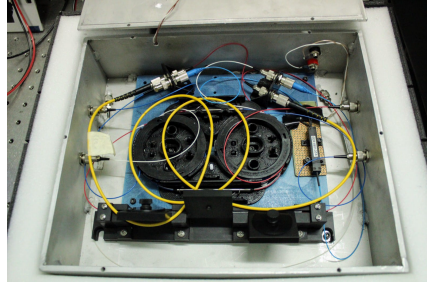


Figura 3.4: Gabinete contenedor de aluminio con el interferómetro dentro del mismo y con la tapa abierta. Para lograr una mayor aislación del ambiente, se dispuso al gabinete dentro de una caja contenedora construida con foamboard, separada del gabinete por una capa de 25 mm de espuma de poliuretano.

3.2 Fibras ópticas

En la actualidad, el canal natural para comunicaciones ópticas terrestres -y que ha permitido un aumento exponencial de la capacidad de transmisión de datos alrededor del planeta- son las fibras ópticas. Estas consisten en un par de capas concéntricas de vidrio de distinto índice de refracción, que guían la luz por reflexión total interna. Al ser un medio sólido transparente, las fibras ópticas tienen la particularidad de alterar la fase global de la luz a la salida cuando son sometidas a una variación en temperatura o una torsión de la misma, ya sea por variaciones del índice de refracción o por la propia dilatación del material. Es por esto que pueden funcionar como buenos sensores de temperatura y presión como se demostró en trabajos previos [38], [39]. La variación de la longitud efectiva de la fibra (L_{eff}) de un interferómetro de Mach-Zehnder con una variación ΔT en temperatura está dada por la siguiente ecuación [38]:

$$dL_{eff}(\Delta T) = \Delta L \left(\frac{dn}{dT} + \frac{1}{\Delta L} \frac{dL}{dT} n_0 \right) \Delta T \quad (3.1)$$

donde ΔL es la diferencia de longitud entre los caminos ópticos, que en el caso del interferómetro con desbalance de caminos en este experimento vale $\Delta L = 0.4$ m. n_0 es el índice de refracción de la fibra, que en el contexto de este experimento se tomó como 1.456, y $\frac{dn}{dT}$ es la variación del índice de refracción con la temperatura que para este tipo de fibras se midió experimentalmente [40] y vale $12.9 \times 10^{-6} 1/^\circ C$. Del mismo experimento se extrajo también la variación de longitud de este tipo de fibras con la temperatura: $\frac{1}{\Delta L} \frac{dL}{dT} = 0.4 \times 10^{-6} 1/^\circ C$. A su vez, es posible también estimar el desfase relativo producido por un cambio en temperatura ΔT por medio de la siguiente ecuación:

$$d\phi(\Delta T) = dL_{eff} \frac{2\pi}{\lambda} \quad (3.2)$$

Usando los valores mencionados y que la frecuencia del láser utilizado fue 193 THz junto con las ecuaciones detalladas se modeló la variación en longitud efectiva y en fase de un interferómetro de Mach-Zehnder. Los resultados se muestran en las figuras a continuación donde se observa que una variación en temperatura de 1.5 °C hace variar la fase 5 ciclos.

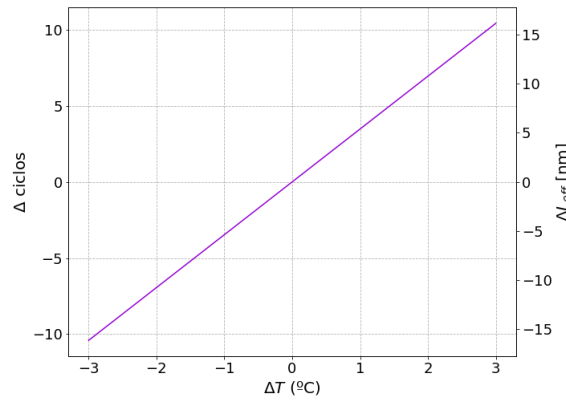


Figura 3.5: Modelo de variaciones producidas en la longitud efectiva (L_{eff}) y fase expresada en número de ciclos en la fibra como consecuencia de fluctuaciones en temperatura.

3.3 Estabilización del interferómetro Mach-Zehnder.

En esta sección se describe el trabajo de caracterización del interferómetro de Mach-Zehnder documentando el mejor contraste posible y estudiando su estabilidad. Esto se hizo para dos distintas configuraciones del interferómetro: balanceado y desbalanceado. Se trabajó con luz intensa usando como fuente de luz el láser ITLA no atenuado, caracterizado en el capítulo anterior.

3.3.1 Interferómetro balanceado.

En primer lugar se estudio la estabilidad del interferómetro de Mach-Zehnder sin desbalance de caminos. Antes de realizar la medición se usó el control de polarización manual para compensar cualquier efecto mecánico residual que hubiera podido generarse en el armado del interferómetro.

En el gráfico 3.6 se muestra como varió la salida del interferómetro balanceado al modificar el entorno en el cual se encontraba el interferómetro. En la región señalizada como 1 el interferómetro se encontraba dentro del gabinete contenedor de aluminio sin la tapa puesta y con el aire acondicionado del laboratorio apagado. Se observa que durante los 40 minutos en los que se encuentra en este entorno fluctúa poco, del orden de 20 %. Luego se procede a encender el aire en modo calefacción y se mantiene la caja abierta. En esta región, designada como región 2 en el gráfico, la fase se vuelve más inestable. Luego de 15 minutos se cambió el modo del aire

acondicionado de calefacción a ventilación y se procedió a realizar una medición de 35 minutos que está marcada como región 3 en el gráfico. Finalmente, sin modificar la configuración del aire acondicionado se puso la tapa de la caja (región 4) y se observó una mejora significativa en la estabilidad del interferómetro. Subsiste una leve deriva, posiblemente consecuencia de la variación en temperatura ya que al haber apagado la calefacción la habitación se comenzó a enfriar, pero son fluctuaciones mucho menores incluso comparando con la medición realizada a temperatura ambiente. De estos resultados se concluye que el gabinete contenedor cumple su función y aísla térmicamente al interferómetro.

En el caso del interferómetro balanceado se espera que ambos caminos, al tener el mismo largo y estar expuestos a la misma fluctuación en temperatura, no cambien su fase relativa. Sin embargo, vemos que la intensidad a la salida fluctúa y parece hacerlo como consecuencia de fluctuaciones en el entorno, ya que fluctúa más cuando está encendido el aire que cuando está apagado. Aproximadamente 50 cm de la fibra del camino 1 se encuentra dentro del *fiber stretcher* por lo que es posible que tarde más en termalizar, generando una diferencia de fase entre los caminos. A su vez, en modo calefacción y ventilación el aire acondicionado sopla aire y al estar la caja abierta esto genera vibraciones diferentes en cada uno de los caminos. Cuando se mueve o torsiona la fibra óptica, esto provoca un cambio en la longitud efectiva de la fibra lo cual modifica el desfase entre los caminos y consecuentemente cambia la intensidad a la salida. Esto también explica por qué las fluctuaciones en la región 3 son mayores a las de la región 4 donde se colocó la tapa de la caja: en esta configuración se evitan corrientes de aire que provocan pequeñas vibraciones en las fibras.

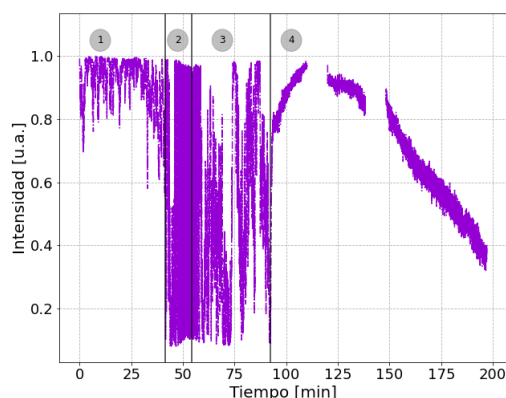


Figura 3.6: Intensidad de luz normalizada a la salida del interferómetro de Mach-Zehnder variando las condiciones del entorno. 1) caja abierta y con aire apagado. 2) caja abierta y aire en modo calefacción. 3) caja abierta y aire encendido en modo ventilación. 4) caja cerrada y aire encendido en modo ventilación.

Luego de caracterizar la estabilidad se estudió el máximo contraste posible del interferómetro balanceado, donde el contraste interferencial, o visibilidad, definido por:

$$C = \frac{I_{max} - I_{min}}{I_{max} + I_{min}} \quad (3.3)$$

En la figura 3.7 se muestra la variación de la intensidad de salida del interferómetro balanceado al mover manualmente la fibra de uno de los caminos. Esta medición fue tomada con el osciloscopio Siglent SDS 1102 CML. Las mediciones se encuentran normalizadas. Esto se hizo para todas las mediciones de intensidad para poder comparar mediciones realizadas con distintos instrumentos. Se observa que cuando está balanceado es posible conseguir un contraste ideal ($C = 1.000 \pm 0.011$). El contraste se calculó a partir de los resultados de medición de voltaje sin normalizarlos. Esta optimización, manual, es estable en el tiempo y se mantiene por días en la medida en que se mantenga su configuración o no se perturbe mecánicamente el dispositivo.

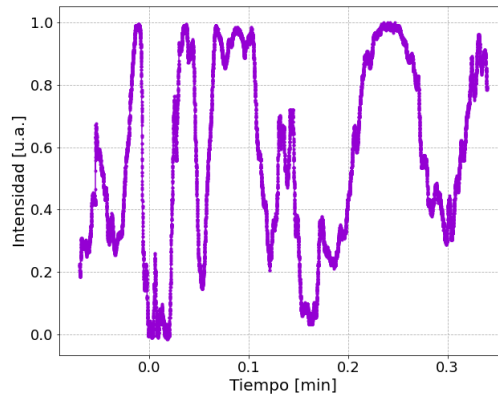


Figura 3.7: Intensidad de luz normalizada a la salida del interferómetro de Mach-Zehnder balanceado. Durante la medición se movió manualmente la fibra de uno de los caminos para cambiar en forma aleatoria el contraste. Se observa que para el interferómetro balanceado es posible lograr un contraste de 1.000 ± 0.011 .

3.3.2 Interferómetro con desbalance de caminos.

Luego de caracterizar el interferómetro balanceado se procedió a introducir un desbalance equivalente a 2 ns entre los caminos del interferómetro, y caracterizar y comparar la estabilidad. En la figura 3.8 se graficó la variación de la intensidad a la salida para el interferómetro balanceado (en violeta) y desbalanceado (en verde), en situaciones de operación similares. En ambas mediciones el interferómetro se encontraba dentro del gabinete cerrado y se encendió la ventilación del sistema de acondicionamiento de aire. Como es esperable, el interferómetro balanceado es significativamente más estable ya que ambos caminos tienen el mismo largo y están expuestos a temperaturas similares. Por otro lado, para la medición realizada con desbalance de caminos, el interferómetro fue significativamente menos estable. Entre las dos

lineas punteadas hay un total de 21 ciclos. Usando estos resultados y el gráfico 3.5, podemos estimar que en los 35 minutos de medición la temperatura varió localmente poco mas de 6°C.

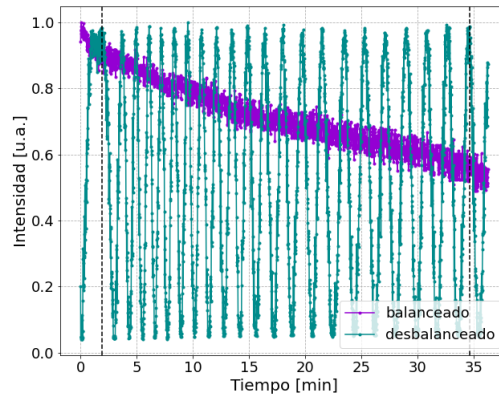


Figura 3.8: Comparación de fluctuaciones en la intensidad de luz normalizada a la salida del interferómetro balanceado (en violeta) ó con un desbalance de caminos de 0.4 m (en verde). Se observa que la medición del interferómetro balanceado es significativamente mas estable que con una diferencia de longitud entre los caminos.

Luego de caracterizar la estabilidad se estudió el contraste del interferómetro desbalanceado. Resulta importante aclarar que nuevamente se maximizó el contraste antes de tomar la medición usando el control de polarización manual. Para calcular el contraste se realizó un histograma de los datos no normalizados, que se muestra en la figura 3.9. La señal tiene una forma sinusoidal por lo que se espera un máximo de cuentas del histograma para el mínimo y máximo. Del histograma se buscaron los picos correspondientes a las excursiones de máxima y mínima de intensidad, a partir de los cuales se calculó el contraste. Se obtuvo un valor de 0.985 ± 0.013 . Es menor que para el caso balanceado donde se obtuvo un contraste ideal de 1.00 ± 0.011 . El contraste puede verse afectado por pérdidas distintas en los brazos del interferómetro, que generan superposición de ondas con distinta amplitud. Pero en última instancia, uno de los factores fundamentales que producen pérdida de contraste en interferómetros balanceados es la longitud de coherencia de la fuente: si la longitud de caminos es comparable o mayor que la longitud de coherencia, el contraste se deteriora. Para estos experimentos puntuales del estudio de la estabilidad se utilizó el láser ITLA, cuyo ancho de línea intrínseco está por debajo de los 50 kHz y por ende una longitud de coherencia superior al kilómetro. Las pruebas posteriores en régimen conteo de fotones se realizaron con un láser DFB sin cavidad externa que tiene una longitud de coherencia de aproximadamente 2 m, con lo cual el contraste en un interferómetro con aproximadamente 0.4 m de desbalance no es óptimo.

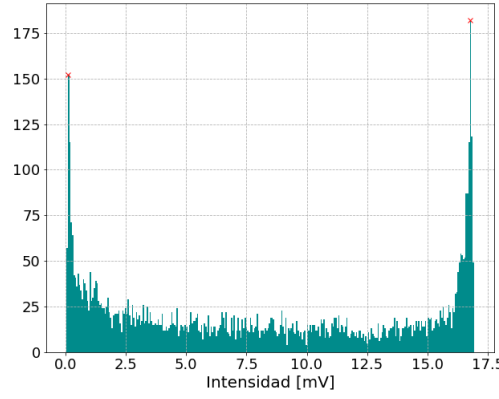


Figura 3.9: Histograma de la intensidad sin normalizar del interferómetro desbalanceado que se usó para calcular el contraste. Con cruces rojas se marcó la posición del máximo y mínimo. El contraste hallado fue de 0.985 ± 0.013 .

3.4 Lazo de estabilización por maximización de intensidad.

El control externo de la fase impuesta por el interferómetro a dos pulsos que ingresan separados temporalmente un tiempo $t = \Delta L_c^n$ se realiza actuando sobre el *fiber stretcher* por medio de un lazo de control implementado en Arduino. Este dispositivo ya estaba operativo en el laboratorio pero se describe en esta sección por completitud.

El algoritmo busca maximizar la señal de una de las salidas del interferómetro, de forma que la fase relativa entre los dos pulsos impuesta por el dispositivo sea nula. Se hace uso de la propiedad periódica y continua de la señal a maximizar. A su vez, si se le aplica una señal de voltaje monótonamente ascendente (descendente) al piezo-eléctrico, la intensidad también tiene el mismo comportamiento periódico, lo que permite llegar a un máximo (mínimo). El algoritmo de estabilización funciona de forma iterativa de manera que el paso k del algoritmo sigue la siguiente ecuación:

$$V_{stretcher}^{(k+1)} = V_{stretcher}^{(k)} + \Omega(\tilde{V})^{(k)} \quad (3.4)$$

donde $\Omega(\tilde{V})^{(k)}$ es el paso del algoritmo y define cuánto se mueve dentro del patrón de interferencia. Se detalla el protocolo de maximización, el de minimización es análogo. El signo de $\Omega(\tilde{V})^{(k)}$, que define en qué dirección se mueve en el patrón, se elige usando la relación entre cada paso con el anterior

$$sign(\Omega(\tilde{V})^{(k)}) = sign(\tilde{V}^{(k)} - \tilde{V}^{(k-1)}) \quad (3.5)$$

donde el primer paso se elige como positivo. El algoritmo se encuentra esquematizado en la figura 3.10 donde se muestra que valores toma el signo de $\Omega(\tilde{V})^{(k)}$ para cuatro pasos.

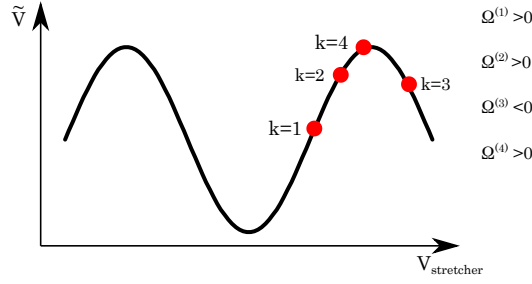


Figura 3.10: Esquema de algoritmo de maximización extraído de [17].

La magnitud de $|\Omega|$ se elige de forma que sea proporcional a la distancia al máximo. Esto se hace porque si se elige un paso muy grande se generan oscilaciones entre puntos cercanos al máximo; entre $\tilde{V}^{(2)}$ y $\tilde{V}^{(3)}$, por ejemplo, pero por otro lado si es muy chico la aproximación a un extremo es muy lenta y puede no estabilizar antes de que la fase fluctúe. Es por esto que al ser proporcional a la distancia, se acerca rápido al máximo y luego no puede alejarse mucho. Luego también en base a las mediciones se modifica el paso mínimo Ω_{min} si tarda mucho en estabilizar ó se achica si oscila demasiado. El valor del paso del algoritmo en el paso k está dado por la ecuación

$$\Omega^{(k)} = \Omega_{min} + \frac{\Omega_{max} - \Omega_{min}}{\tilde{V}_{max} - \tilde{V}_{min}} (\tilde{V}_{max} - \tilde{V}^{(k)}) \quad (3.6)$$

3.4.1 Implementación del algoritmo de maximización.

Se implementó el algoritmo de maximización sobre el interferómetro usando el Arduino Mega2560. Para aplicar el algoritmo de maximización el Arduino necesita leer en simultáneo la intensidad de salida del interferómetro. También necesita registrar la máxima y mínima intensidad antes de comenzar el protocolo. Para eso primero hace un barrido enviando una señal triangular al *fiber stretcher* y registra los valores de intensidad máximo y mínimo obtenidos sobre la señal del fotodiodo, y luego devueltos por el fotodiodo y luego comienza a estabilizar en un máximo. Ya que el Arduino lee y guarda la señal de salida del interferómetro, en estas mediciones se lo utilizó como instrumento de medición en reemplazo del osciloscopio. En la figura 3.11 se muestran los resultados de la medición (a la derecha) y de la señal enviada al *stretcher* a la izquierda. En esta medición el barrido duró 10 minutos. El algoritmo actúa cada 50 ms y se observa que es capaz de mantener estable en un máximo la salida del interferómetro con fluctuaciones menores al 10 %.

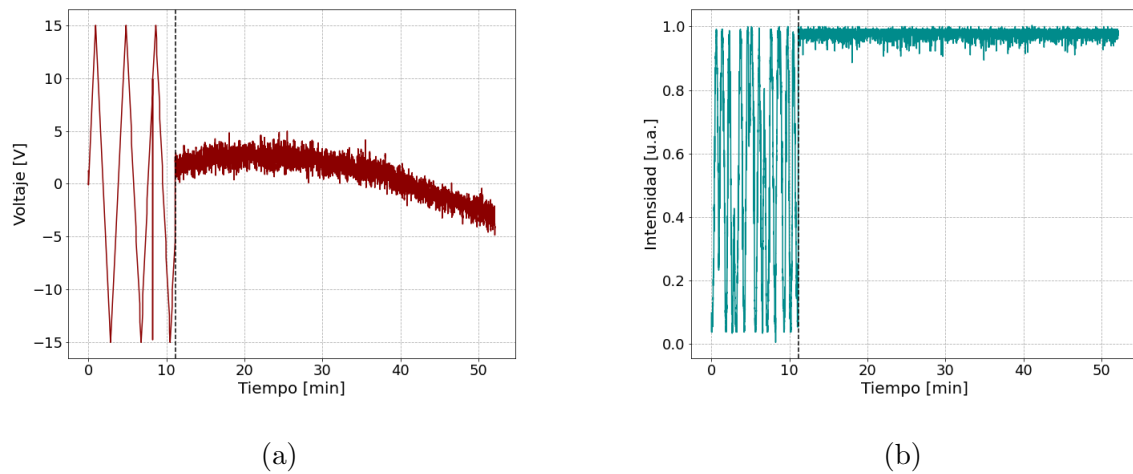


Figura 3.11: Estabilización del interferómetro con desbalance de caminos usando el algoritmo de maximización de Arduino. (a) Señal enviada al *fiber stretcher* desde el Arduino. (b) Intensidad de salida del interferómetro normalizada registrada con el Arduino.

Esta medición fue realizada sin control activo de temperatura. Luego de montar la celda Peltier dentro de la caja se repitió esta medición y para estas escalas temporales no se pudo apreciar una mejora ni en la estabilización ni una reducción en el trabajo realizado por el *stretcher*. Esto es consecuencia de que el Arduino corrige más rápido de lo que deriva la temperatura y por ende las fluctuaciones en temperatura no afectan la estabilidad cuando está el algoritmo de maximización funcionando. Sin embargo lo que se pretende reducir con el control de temperatura son las derivas grandes de diferencia de caminos generadas en escalas temporales de un ciclo diurno. Además, las variaciones en temperatura pueden afectar el contraste, como se detallará en la próxima sección. Es por esto que si bien en mediciones cortas la implementación del control activo de temperatura no implica una mejoría, sí reduce la necesidad de corregir el contraste del interferómetro moviendo el control de polarización manual entre mediciones de distintos días.

3.4.2 Contraste y temperatura.

Variando las condiciones de temperatura del entorno del interferómetro se observó que el contraste del mismo fluctúa con la temperatura. En la figura 3.12 se muestra la variación de intensidad a la salida del interferómetro de Mach-Zehnder con una fuente de luz intensa al enviar una señal triangular al *fiber stretcher* que modifica gradualmente la fase. El interferómetro se encontraba dentro del gabinete contenedor de aluminio a temperatura ambiente y se midió la salida del interferómetro usando el controlador Arduino. En este caso para calcular el contraste no se normalizaron los datos. A la derecha se muestra un histograma de esta medición que se usó para calcular el contraste. Se encontró que el contraste en estas condiciones era de (0.9137 ± 0.018) .

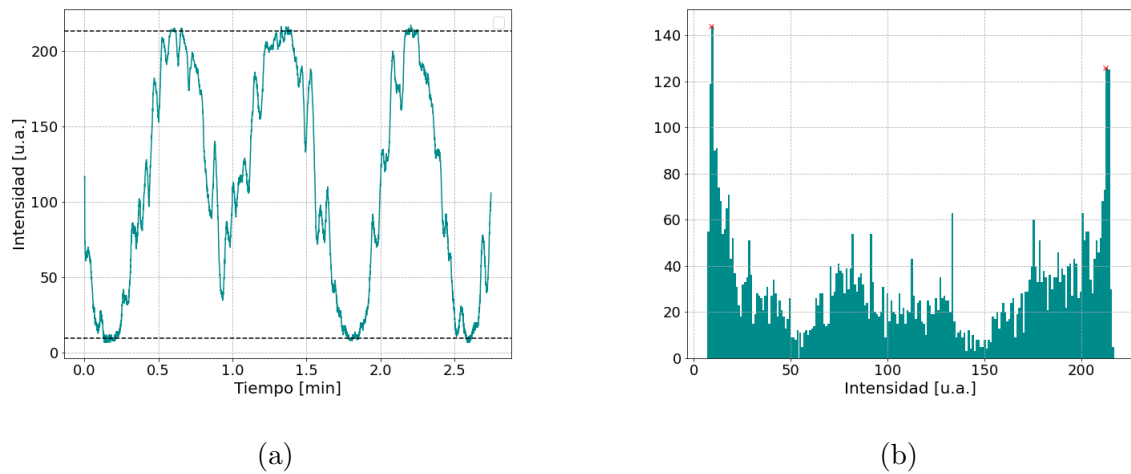


Figura 3.12: Medición del contraste haciendo un barrido de la fase entre los caminos con el interferómetro a temperatura ambiente, las líneas punteadas representan el mínimo y máximo hallado del histograma. (a) Variación de intensidad a lo largo del tiempo. (b) Histograma de la medición.

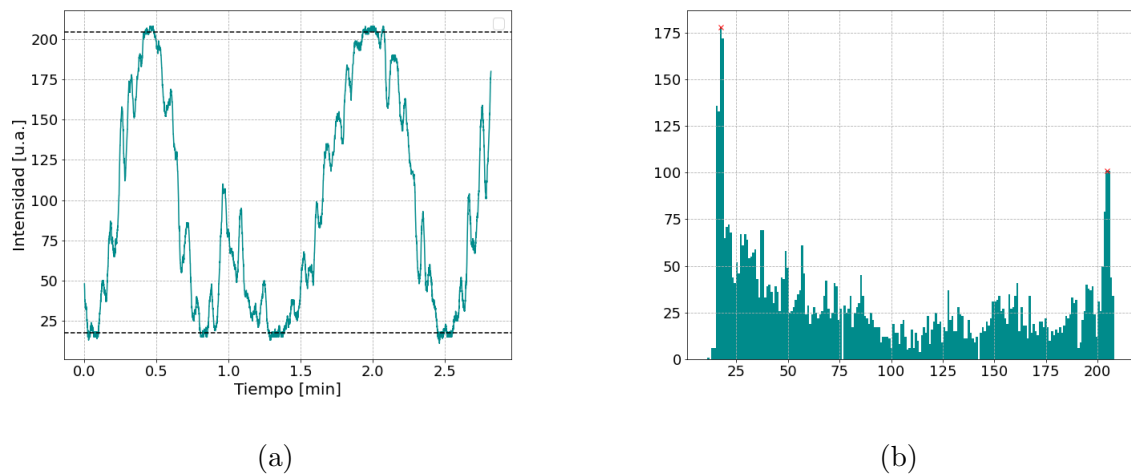


Figura 3.13: Medición del contraste haciendo un barrido de la fase entre los caminos con el interferómetro con el aire acondicionado encendido en modo calefacción, las líneas punteadas representan el mínimo y máximo hallado del histograma. (a) Variación de intensidad a lo largo del tiempo. (b) Histograma de la medición.

Por otro lado en la figura 3.13 se muestra la medición de la intensidad a la salida del interferómetro en condiciones análogas a la medición anterior pero ahora con la calefacción prendida. Se halló que el contraste bajo a un valor de (0.8432 ± 0.0164) , que es menor al contraste para cuando el interferómetro se encontraba a temperatura ambiente, es decir, que el contraste del interferómetro varía al cambiar la temperatura. Esto resulta razonable ya que al cambiar la temperatura la fibra puede sufrir modificaciones que afecta la polarización de

cada fibra de manera distinta, introduciendo una diferencia en polarización entre los caminos de la fibra.

En el gráfico en la figura 3.14 se grafican ambos histogramas sobre la misma figura. Se observa que grandes variaciones en temperatura modifican el contraste. Es por esto que en mediciones de distintos días es necesario cambiar la polarización de una de las fibras antes de comenzar cada medición, lo cual significa que hay que abrir la caja. En este sentido tener un control de temperatura es beneficioso ya que estabiliza el contraste al estabilizar la temperatura y ya no es necesario modificar la polarización. En la próxima sección se describe el sistema de control construido e implementado.

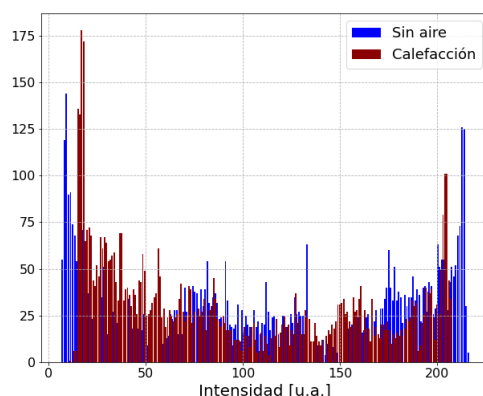


Figura 3.14: Histograma de medición de intensidad al barrer la fase entre ambos caminos para una medición a temperatura ambiente y con calefacción encendida.

3.5 Control de temperatura

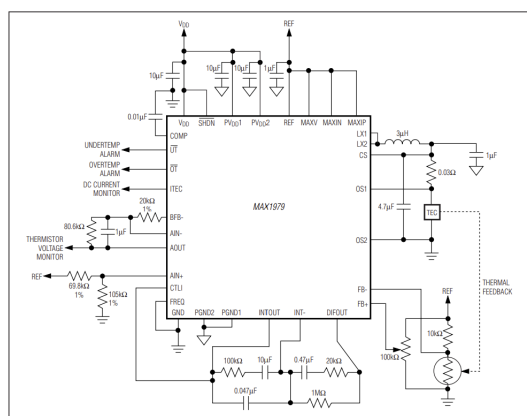
Uno de los objetivos principales de este trabajo fue poder controlar la temperatura del receptáculo del interferómetro, por medio de un lazo de realimentación. Para ello, luego de caracterizar la fuente de luz y la estabilidad del interferómetro se diseñó e incluyó dentro del interferómetro un control de temperatura basado en el componente MAX 1979 [41]; un módulo de control de temperatura para dispositivos de enfriamiento termoeléctrico (TEC) Peltier.

3.5.1 Diseño e implementación

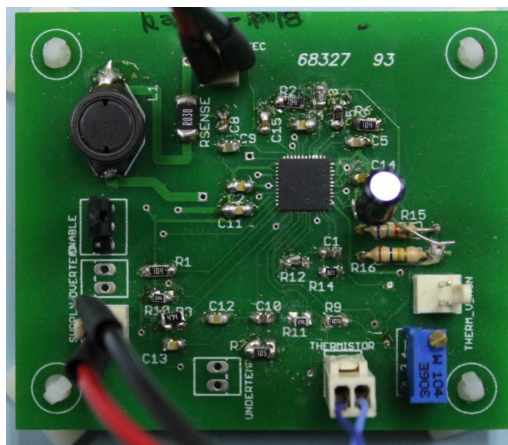
El controlador MAX 1979 permite entregar hasta 6A a un enfriador termoeléctrico usando modulación PWM sobre una fuente de conmutación. Tanto el filtro pasabajos de alimentación del TEC como los límites de voltaje y corriente, y el circuito del lazo de control se definen externamente, lo que lo hace flexible y versátil, pudiendo adaptarse a distintas cargas térmicas y retardos en la señal de control. Un esquema del circuito de dicho módulo de control se encuentra en la figura 3.15a. A la derecha de esta figura (figura 3.15b) se muestra en esquema

CAPÍTULO 3. INTERFEROMETRÍA DE UNA ÚNICA FUENTE EN DISPOSITIVOS DE FIBRA ÓPTICA

del circuito diseñado e implementado en el laboratorio. El componente MAX1979 es unipolar; solo enfría (o calienta). El circuito cuenta también con un *switch* que permite encender o apagar el control de temperatura.



(a)



(b)

Figura 3.15: Diseño de circuito del control de temperatura. (a) Modelo de circuito usado en los controles de temperatura MAX 1979. Figura extraída del manual [41]. (b) Foto del circuito diseñado e implementado en el laboratorio basado en el modelo MAX 1979.

El lazo de control del módulo de control de temperatura funciona con un lazo PID. Los PID (Proporcional - Integral - Derivativo) son un tipo de instrumento utilizado para regular temperatura, flujo, velocidad, entre otros procesos que requieran control del sistema. Es un método que consiste en forzar una realimentación al sistema, para lograr que el mismo iguale un punto de trabajo definido externamente. El valor de la magnitud de esa realimentación es función de los parámetros de control [42]. Es un lazo cerrado de control en el cual se toma una señal error que es equivalente a la diferencia entre la señal de salida del circuito y el valor fijado y se usa esta señal error para modificar el sistema y llevarlo al valor deseado. Los PID tienen, como su nombre la indica, tres pasos. El primero es una parte proporcional que corrige la salida por medio de un valor proporcional a la del error. Multiplica la señal error por un factor que se denomina ganancia y envía eso como corrección. Existen sistemas de control que solo cuentan con la parte proporcional. El problema con este tipo de sistemas es que si la ganancia es muy pequeña nunca se llega al valor deseado ya que el sistema fluctúa antes de que llegue a estabilizar pero si es muy grande se acerca al valor fijado y oscila alrededor del mismo. Debido a esto se introduce un segundo paso que es denominado paso integral. Este paso intenta compensar los problemas que tiene el paso anterior. Aquí lo que hace el lazo de control es introducir una corrección que se relacione al error acumulado. De esta manera el sistema tiende a ir a un error acumulado nulo. El problema con esto es que puede resultar en un sobresalto, es decir, que el sistema estabilice a un valor por encima del deseado. Finalmente se introduce una corrección denominada como derivable en el cual se pretende minimizar el

sobresalto. Es un factor que disminuye la variable de control si el sistema crece muy rápido. La respuesta derivada es proporcional a la tasa de cambio de la variable de control. Se debe tener en cuenta que este tipo de lazos de control siguen teniendo problemas, por la parte de la derivada el sistema se vuelve inestable si, por ejemplo, la señal de entrada resulta muy ruidosa. En la figura 3.16 se muestra un esquema del lazo PID implementado en el control de temperatura. En la entrada (*In*) entra la señal error que es la diferencia entre la caída de potencial del termistor y la caída de potencial por el potenciómetro. A la salida (*Out* en el esquema) se envía la señal de corrección generada por el lazo PID. Siguiendo el diseño sugerido en [41], se variaron empíricamente los valores de resistencia del integrador (R_3 en la figura 3.16) hasta eliminar las oscilaciones de la temperatura. Siguiendo este esquema se muestra en la figura 3.17 el diagrama de Bode de dicho circuito.

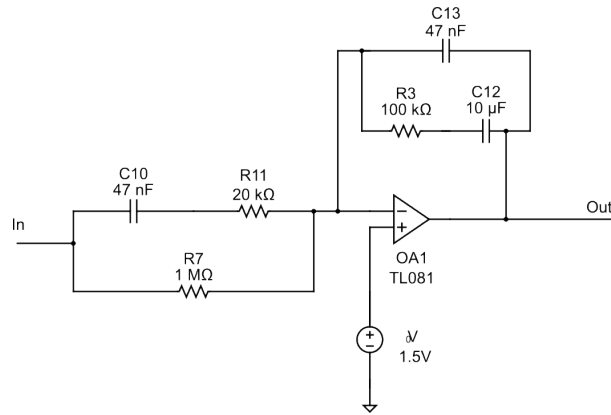


Figura 3.16: Esquema del circuito PID utilizado en el control de temperatura diseñado.

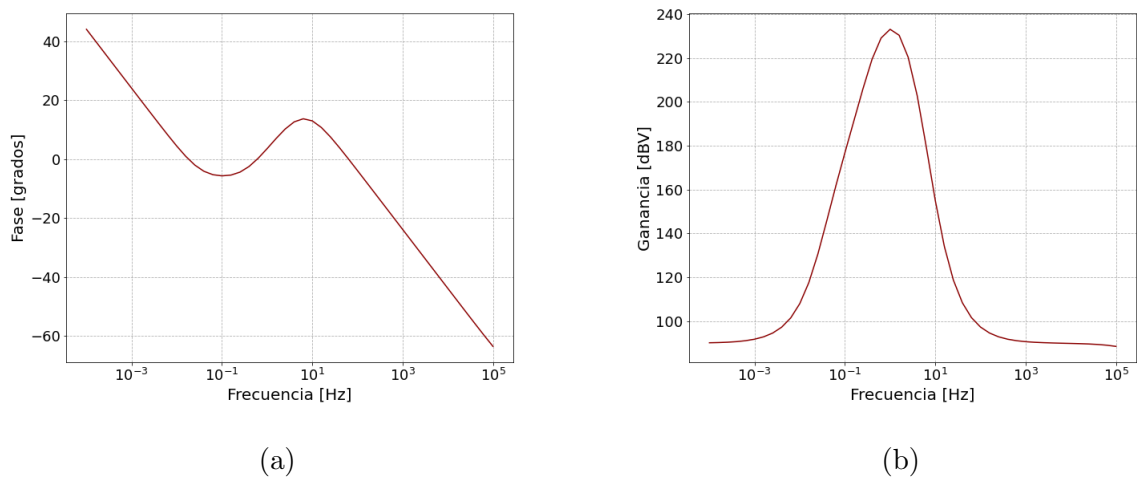


Figura 3.17: Diagramas de bode del lazo PID del control de temperatura.

Este circuito es alimentado por una fuente continua de 5V y esta conectado a una Peltier que esta colocada del lado de afuera de la tapa del gabinete contenedor y se usa para enfriarlo. Las Peltier o refrigerador termoeléctrico (TEC) son dispositivos que generan una

diferencia de temperatura, enfriándose de un lado y calentándose del otro, cuando se hace pasar una corriente eléctrica por ellos. Como se diseñó el control de temperatura para enfriar el gabinete contenedor del interferómetro, se colocó la cara que enfría en contacto con la tapa del receptáculo y del lado caliente se colocó un disipador pasivo para quitar calor al sistema completo. Como sensor de temperatura se utilizó un termistor NTC de 10 k Ω adherido al lado interno de la tapa de la caja. Los termistores son buenos elementos de detección de temperatura. Están compuestos por un material semiconductor cuya resistencia R_T varía cuando está expuesto a cambios en temperatura. La relación entre la resistencia de un termistor y la temperatura esta dada por la ecuación de Steinhart & Hart [43].

$$\frac{1}{T} = A + B \ln(R_T) + C(\ln(R_T))^3 \quad (3.7)$$

Los coeficientes de la ecuación de Steinhart & Hart para un termistor de 10 k Ω son: $A = 1.125308852122 \times 10^{-3}$, $B = 2.34711863267 \times 10^{-4}$ y $C = 8.5663516 \times 10^{-8}$.

El controlador con MAX1979 implementa un lazo PID para estabilizar la temperatura, y usa la diferencia de caída de tensión sobre la resistencia del termistor con la caída sobre una resistencia ajustable externamente (el *setpoint*), en una configuración típica de puente resistivo. Para evitar que ruidos eléctricos externos afecten el comportamiento del sistema, todas las entradas y salidas de monitoreo están aisladas usando amplificadores operacionales en modo seguidor (*buffered input/output*). Adicionalmente, se implementó un circuito conformador de señal de salida buffereada de la caída de tensión sobre el termistor, de forma de obtener una señal de monitoreo que se comporte de manera aproximadamente lineal con la variación de temperatura. A continuación en la figura 3.18 se muestra un modelo simplificado del circuito de conformación de la señal de monitoreo de temperatura. La función del mismo es obtener una señal de monitoreo “linealizada” a partir de la caída de tensión en el termistor. Como se aprecia de la ecuación 3.7 la relación entre temperatura y resistencia en estos dispositivos no es lineal. Se encuentran circulados en la figura con distintos colores los valores de referencia que luego se usaron para caracterizar y estudiar el funcionamiento del instrumento. V_{ref} es el voltaje de referencia provisto por el propio circuito integrado. Es una señal estable de 1.5 V, que varía poco más de 1 mV ante variaciones de 1 volt de la tensión de alimentación. V_{mon} es la señal que permite monitorear el valor y la estabilidad de la temperatura sobre el punto de sensado. V_{pot} es la caída de potencial por el potenciómetro que se usa para fijar la temperatura y V_{th} es la caída de voltaje por el termistor. La señal error está dada por la diferencia entre V_{pot} y V_{ref} de forma que la diferencia de voltaje se multiplica por 50 (factor de ganancia), y a partir de esta señal de error se aplica una corrección a la corriente de alimentación de la celda Peltier consistente en una combinación de términos proporcional, integrador y derivativo de dicha señal de error. Estos potenciales se relacionan entre si por la ecuación

$$V_{\text{mon}} = \left(1 + \frac{R_{14}}{R_{12}}\right) \frac{R_{16}}{R_{15} + R_{16}} V_{\text{ref}} - \frac{R_{14}}{R_{12}} V_{\text{th}}. \quad (3.8)$$

También es posible calcular R_T usando los potenciales V_{th} y V_{ref} como se muestra a continuación:

$$R_T = \frac{R_9 V_{th}}{V_{\text{ref}} - V_{th}}. \quad (3.9)$$

Para las resistencias se usaron los siguientes valores:

$$R_9 = 10 \text{ k}\Omega, \quad R_{12} = 22 \text{ k}\Omega, \quad R_{14} = 82 \text{ k}\Omega, \quad R_{15} = 68 \text{ k}\Omega, \quad R_{16} = 100 \text{ k}\Omega \quad (3.10)$$

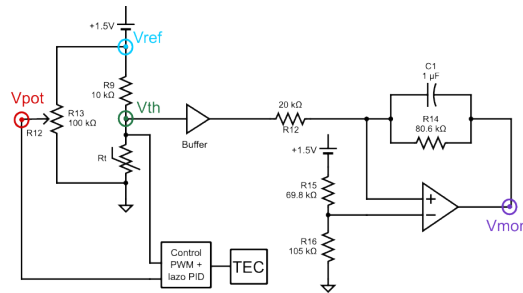


Figura 3.18: Modelo simplificado del circuito de control de temperatura. V_{ref} valor de referencia equivalente a 1.5 V. V_{mon} señal de monitoreo. V_{pot} es la caída de potencial por el potenciómetro. V_{th} es la caída de potencial por el termistor. R_T representa la resistencia del termistor y TEC la Peltier. La señal error esta dada por la diferencia entre V_{th} y V_{pot} y a partir de esta señal y del lazo de ganancia proporcional, integrador y derivador, el dispositivo controla la corriente regulando la señal PWM sobre los transistores MOSFET de salida.

3.5.2 Caracterización

Una vez diseñado el control de temperatura se buscó caracterizar su funcionamiento. Para ello se midió la variación de V_{ref} , V_{mon} , V_{pot} y V_{th} en el tiempo. Estos potenciales se midieron usando el osciloscopio digital DPO7054 Tektronix habiendo colocado de un lado de la tapa de aluminio de la caja la Peltier con el lado que enfría en contacto con la tapa y del otro el termistor. Se repitió la medición para distintas temperaturas. Para bajar (subir) la temperatura fijada es necesario girar la perilla del potenciómetro en sentido antihorario (horario). Los resultado de una de las mediciones se muestra en la figura 3.19. En esta medición el sistema estabilizó a $(21.2 \pm 1) ^\circ\text{C}$. Esta temperatura fue medida con un termómetro con precisión de $1 ^\circ\text{C}$ colocado sobre la tapa. En rojo se graficó el valor de V_{pot} que se espera no varíe a lo largo de la medición. La línea punteada representa el valor promedio de V_{pot} al inicio antes de desconectarlo. La tapa se estabiliza en temperatura en menos de 15 minutos. Esto también ocurrió para todas las otras mediciones. A su vez, se observa que el valor de V_{th} tiende al valor de V_{pot} como se espera.

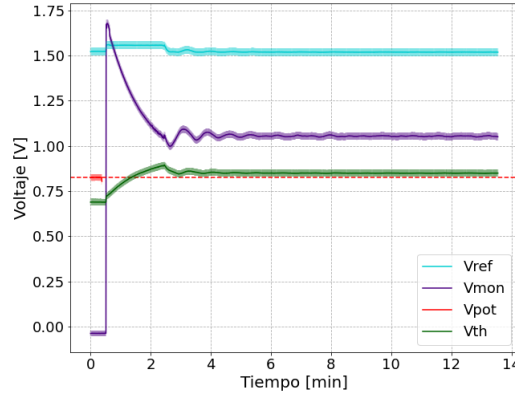


Figura 3.19: Caracterización del control de temperatura. En esta medición el sistema estabilizó a $T = (21.2 \pm 1) ^\circ\text{C}$. V_{pot} se midió solo al principio y luego se desconectó por lo que la señal cae a 0. V_{th} tiende a V_{pot} al estabilizar.

Por otro lado también se buscó verificar que se cumpla la ecuación 3.8 para la medición mostrada arriba. Para cada valor medido se tomó el valor de V_{ref} y V_{th} y se calculó V_{mon} usando la ecuación y se lo graficó en rosa. En violeta se muestra el valor de V_{mon} medido experimentalmente. Se observa que el valor experimental y del modelo tienen comportamientos análogos y que el valor predicho por el modelo se acerca al valor medido.

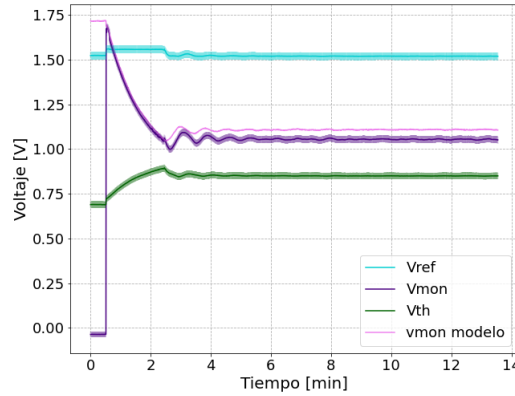


Figura 3.20: Verificación experimental de la relación entre los potenciales. V_{mon} modelo se calcula a partir de la ecuación 3.8 y usando los valores medidos de V_{ref} y V_{th} .

3.5.3 Ecuación de Steinhart & Hart

Se buscó también estudiar el termistor y calcular experimentalmente los coeficientes A,B y C de la ecuación de Steinhart & Hart. Para eso en cada una de las mediciones se registró la temperatura final con el termómetro. Estas medidas se expanden en el rango de temperaturas en el cual se trabajará luego. Se calcularon V_{ref} , V_{pot} y V_{mon} como el promedio de los últimos

500 datos medidos, que equivale a los últimos 3.5 minutos de medición. Una vez obtenidos los valores promediados de los potenciales se calculó R_T a partir de las mediciones. Para ello primero se calculó V_{th} usando la ecuación 3.8 y los valores medidos de V_{mon} y V_{ref} . Luego se usó ese V_{th} y el valor medido de V_{ref} para calcular R_T usando la ecuación 3.9. Los resultados de las mediciones se encuentran graficadas en la figura 3.21. Primero se intentó ajustar los resultados con la ecuación de Steinhart & Hart y hallar los coeficientes experimentalmente. Sin embargo se obtenían parámetros de ajuste con un error mayor al 100 %. Esto ocurre porque el modelo incluye un término proporcional a $\log(R)^3$, que para variaciones chicas de temperatura no es relevante: este término se vuelve relevante para rangos de temperaturas mayores. Como solo se estudiaron temperaturas menores a 40 °C no es necesario este parámetro. Se procedió a ajustar los datos con la ecuación de Steinhart & Hart fijando $C = 0$ y calculando del ajuste los coeficientes A y B. El ajuste se hizo con los datos de temperatura en Kelvin y las resistencias en Ω . Del ajuste se obtuvieron los valores de los coeficientes: $A = (1.53 \pm 0.20) \times 10^{-3}$ y $B = (1.97 \pm 0.22) \times 10^{-4}$. En violeta se muestra el ajuste de los datos experimentales y en azul se muestra la temperatura calculada con los valores de A,B y C del fabricante. El modelo ad-hoc es adecuado para modelar el comportamiento de los resultados en este rango de temperaturas. Se observa que usando los coeficientes del fabricante se obtiene una curva que difiere significativamente de los datos por lo que es preferible usar los coeficientes hallados mediante el ajuste en este rango.

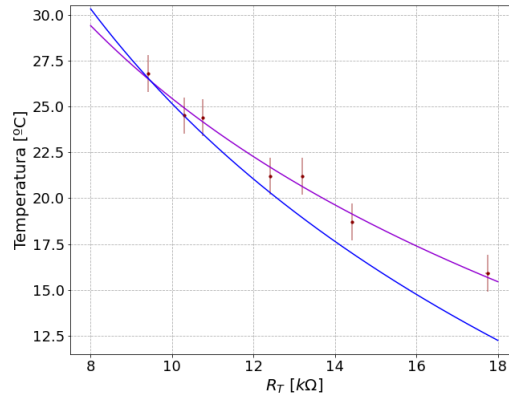


Figura 3.21: Relación de la temperatura con la resistencia del termistor R_T . Se verifica que cumple la relación de Steinhart & Hart. En azul se muestran los valores de temperatura obtenidos con los coeficientes del fabricante. En rojo se muestran los resultados experimentales y en violeta el ajuste de las mediciones con la ecuación de Steinhart & Hart (ec 3.7). Del ajuste se obtuvo $A = (1.53 \pm 0.20) \times 10^{-3}$ y $B = (1.97 \pm 0.22) \times 10^{-4}$.

Luego de caracterizar el termistor se buscó encontrar una relación que permitiese calcular la temperatura fijada a partir de V_{mon} . No se usan los otros valores ya que por cómo está diseñada la placa, V_{mon} es el valor más fácil de medir y a su vez es el más estable. En la

figura 3.22 se muestra la relación simulada entre la temperatura y V_{mon} calculada a partir de las ecuaciones 3.8, 3.9 y la parametrización del modelo de S & H usando los coeficientes del fabricante. Se observó que en el rango de temperatura ambiente (menor a 40°C) la relación resulta bastante lineal.

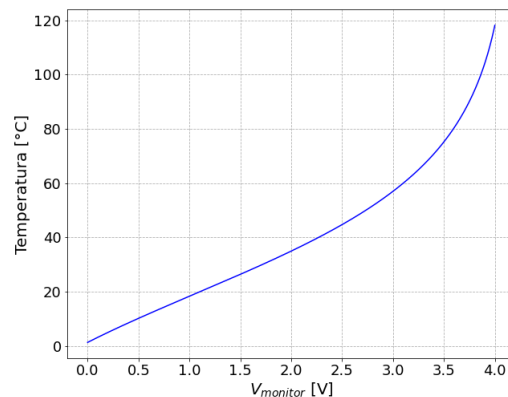


Figura 3.22: Dependencia teórica de la temperatura con el potencial denominado V_{mon} . Se observa que en el rango de temperaturas estudiado la relación puede ser aproximada por una lineal.

Se usaron los resultados experimentales para determinar si es posible aproximar la relación por una ecuación lineal. Los resultados experimentales junto con el ajuste lineal de los mismos se encuentra graficado en rojo en la figura 3.23. En azul se graficó el valor de temperatura calculado a partir de V_{mon} usando los valores experimentales de los coeficientes A,B y C y usando $V_{ref} = 1.5$ V. Del ajuste de los datos experimentales se obtuvo la siguiente relación: $T = (12.3 \pm 1.4) \text{ K/V } V_{mon} + (280.6 \pm 1.6) \text{ K}$. Del gráfico se observa que resulta acorde aproximar la relación por una función lineal en el rango de temperaturas de interés: entre 10 °C y 40 °C, y se obtiene una sensibilidad de aproximadamente 0.012 grados por milivolt. Esto permite determinar sin necesidad de usar un termómetro la temperatura a la cual estabilizó el sistema. Resulta importante destacar que para poder estabilizar en temperatura la temperatura fijada debe ser menor a la temperatura ambiente ya que el sistema solo enfría y no puede calentar. Asimismo, hay que tener en cuenta que la Peltier enfría de un lado pero a costa de entregarle calor al otro lado, por lo que hay un límite de cuánto es capaz de enfriar, ya que si la demanda frigorífica es grande, la cara caliente puede empezar a transmitir calor a través del dispositivo, perdiendo eficiencia rápidamente y haciendo que el sistema completo aumente la cantidad de calor en vez de quitarla.

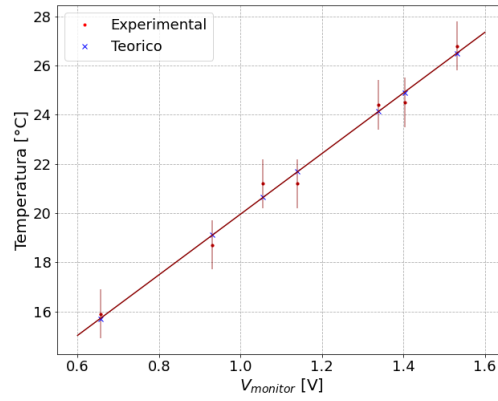


Figura 3.23: Relación experimental entre temperatura y V_{mon} . Los datos fueron ajustados por una lineal. Se obtuvo la siguiente relación: $T = (12.3 \pm 1.4) \text{ K/V } V_{mon} + (280.6 \pm 1.6) \text{ K}$. En azul se graficaron los valores predichos por el modelo usando los coeficientes de Steinhart & Hart hallados experimentalmente.

3.5.4 Caracterización sobre el interferómetro.

Una vez caracterizado el control de temperatura y el interferómetro por separado, se buscó estabilizar en temperatura al interferómetro con desbalance de caminos. El montaje experimental utilizado para realizar estas mediciones se muestra en el esquema 3.24.

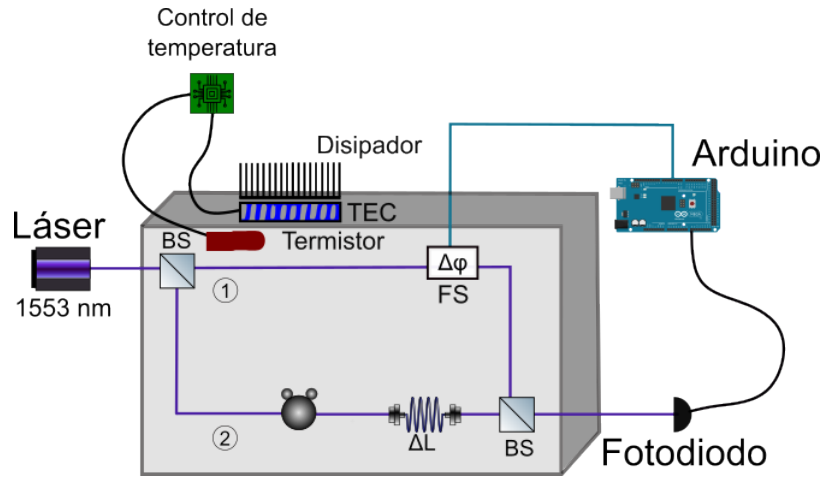


Figura 3.24: Esquema experimental del interferómetro dentro del gabinete de aluminio con el control de temperatura. Del lado de adentro sobre la tapa se colocó el termistor y del lado de afuera la Peltier con un disipador arriba.

Se midió la intensidad a la salida del interferómetro antes y después de encender el control de temperatura. Los resultados de esta medición se muestran en la figura 3.25. Esta medición fue realizada sin el lazo de Arduino funcionando. La intensidad de la medición esta normalizada. A los 20 minutos de comenzada la medición se encendió el control de temperatura.

Este momento está marcado en la figura por una línea vertical violeta. Se observa que hay un brusco cambio en la fase causado por el cambio en temperatura. Justo después de encender la Peltier la fase cambia más rápidamente que antes por un ciclo y luego se ve que a medida que estabiliza la temperatura el periodo del ciclo de franjas se vuelve cada vez más largo. Esto ocurre porque antes del encendido del control de temperatura había fluctuaciones en temperatura que provocaron fluctuaciones en fase que, ya con la Peltier funcionando disminuyeron considerablemente volviendo al interferómetro más estable. Se observa que a partir del minuto 55 de la medición, el sistema llega a un valor constante de temperatura, que se mantiene en un rango dado por la sensibilidad del sistema: esto se manifiesta en el hecho de que la intensidad no llega a un mínimo (condición de interferencia destructiva) sino que evoluciona en forma errática en una condición intermedia.

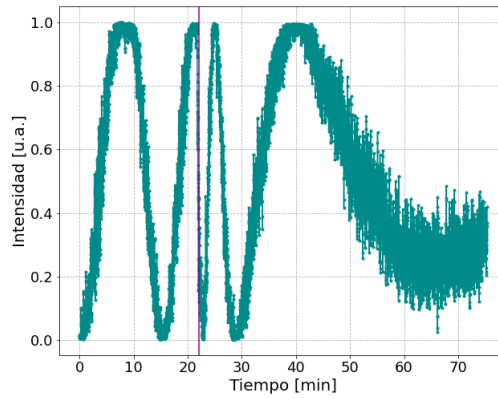


Figura 3.25: Medición de la intensidad a la salida del interferómetro desbalanceado. La intensidad está normalizada. A los 20 minutos del comienzo de la medición se encendió el control de temperatura. Este momento está señalado sobre la figura con una recta vertical violeta. Se observa que el interferómetro se vuelve más estable cuando se estabiliza la temperatura.

A partir del modelo y el cálculo de la variación de camino dependiente de la temperatura obtenido en la sección 3.2, y asumiendo según la figura 3.25 que podemos mantener estable en aproximadamente 0.2 del ciclo óptico, estimamos la variación de temperatura remanente del sistema por debajo de los 50 mK, que consideramos aceptable dadas las dimensiones del gabinete.

A continuación se usará este interferómetro para la detección de estados fase codificada en pulsos *time-bin*, en el régimen de conteo de fotones. La estabilización activa del interferómetro también se realiza en régimen de conteo.

Capítulo 4

Aplicación a QKD

En este capítulo se describe la implementación del protocolo de generación y detección de señales *time-bin*. En primer lugar se describe la optimización del sistema de generación de pulsos. Luego se muestra la implementación del mismo para generar dos estados *time-bin* con fase $\varphi = 0$ y $\varphi = \pi$, a modo de demostración de la capacidad de control de los estados adquirida.

4.1 Implementación experimental de protocolo de QKD en fibra óptica.

Para generar y detectar la interferencia de estados *time-bin* se utilizó el montaje experimental que se muestra en la figura 4.1. Se generaron dos pulsos separados temporalmente por un tiempo Δt . Al pulso que entra primero al interferómetro se lo denomina $|e\rangle$ (*early*) y al siguiente $|l\rangle$ (*late*) y se llama símbolo a un par de pulsos $|e\rangle$ y $|l\rangle$. Si se trabaja con luz intensa y se envían dos pulsos al interferómetro, en el primer *splitter* la señal se divide en dos, y se obtienen dos copias del par de pulsos viajando por cada camino. En el caso de luz de pocos fotones, los pulsos representan la distribución de probabilidad de los fotones y la mitad de las veces los fotones irán por el camino 1 y la otra mitad irán por el otro. De aquí cuando se mencione que se envía un pulso de luz de pocos fotones al interferómetro se hace referencia a que la distribución de probabilidad de los fotones enviados tiene la forma de un pulso con las características deseadas ya que no podemos hablar de un fotón que se divide en dos caminos. De esta forma, al enviar un par de pulsos al interferómetro se espera obtener 3 pulsos a la salida del mismo, como se muestra en el esquema, donde el pulso (bin) central muestra la interferencia del pulso $|e\rangle$ proveniente del camino corto con el pulso $|l\rangle$ que transitó el camino corto. Esta interferencia sólo ocurre si la diferencia temporal entre los pulsos Δt coincide con la diferencia temporal dada por la diferencia de caminos. Para lograr esto se usa el interferómetro desbalanceado con $\Delta L = 40$ cm de fibra óptica monomodo, que equivale a una diferencia temporal de 2 ns.

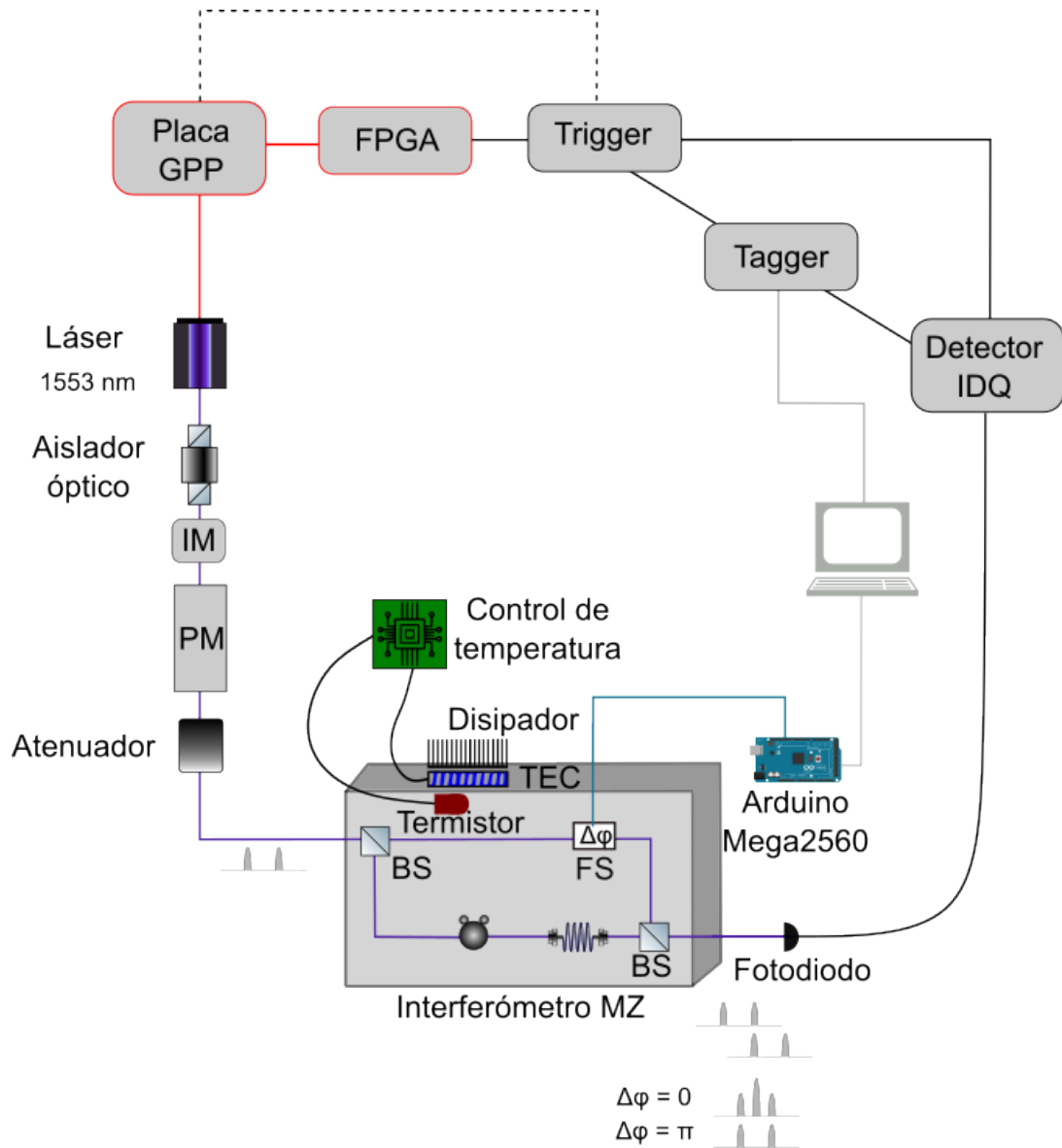


Figura 4.1: Esquema experimental utilizado para la implementación del protocolo de QKD en fibra óptica. Se usa un láser de 1550 nm controlado por la placa FPGA y la placa GPP para generar dos pulsos de luz intensa separados $\Delta t \approx 2$ ns que luego son atenuados para obtener luz de pocos fotones. Los fotones se envían al interferómetro donde los fotones del pulso $|e\rangle$ que fue por el camino largo interfieren con los del pulso $|l\rangle$ que fueron por el camino corto, y a la salida se espera que los fotones tengan una distribución de 3 pulsos. La salida del interferómetro, y en particular la intensidad registrada (o probabilidad de detección) en el pulso o *time-bin* central, se mide usando un detector de pocos fotones de ID Quantique. El detector envía una señal al *tagger* cuando le llega un pulso. A su vez, el *tagger* le envía a la PC el tiempo de llegada de cada fotón al detector. Por otro lado la PC recibe la señal y realiza un protocolo de maximización con el arduino y el *fiber stretcher*. El interferómetro se encuentra dentro de un gabinete contenedor de aluminio para aislarlo térmicamente del entorno. Un termistor ubicado sobre la tapa, del lado interno, registra la temperatura. El sistema de control de temperatura descrito en la sección 2 actúa sobre la celda Peltier ubicada en la cara externa de la tapa del gabinete, y estabiliza la temperatura interna.

Si entonces se envían dos pulsos separados $\Delta t = 2$ ns entre sí al interferómetro es posible hacer interferir los fotones y cambiar la fase usando un mecanismo accionado externamente, por ejemplo el *fiber stretcher*. Para esta caracterización y demostración se utilizó el fiber stretcher para seleccionar la fase de los estados, sin embargo su respuesta temporal es demasiado lenta (en el rango de los kHz) para generar una codificación eficiente. Por lo tanto, en una aplicación real de QKD se utilizará un modulador de fase electroóptico de alta velocidad (ancho de banda de 10 GHz). El fiber stretcher se seguirá utilizando, pero únicamente para el control activo de la fase global del interferómetro.

La implementación del protocolo de QKD puede dividirse en dos partes; generación de los pulsos, que es la parte que correspondería a Alice, y detección de los pulsos, que es la parte de Bob del armado. En este trabajo se buscó trabajar únicamente sobre la parte de Bob del experimento.

Para la generación de los pulsos se generan dos pulsos con luz intensa y luego se los atenúa para obtener luz tenue y estar en las condiciones de experimentos de codificación cuántica de claves. Para generar los pulsos de luz se envía una señal eléctrica cuadrada al láser que le indica que emita luz durante dos ventanas temporales separadas Δt . Para generar la señal eléctrica se usó una placa de desarrollo con un chip FPGA. Como por sí solo este dispositivo no puede generar señales tan rápidas, se usó la misma para controlar el Generador de Patrones de Pulsos (GPP) construido ad-hoc en el Laboratorio de Óptica Cuántica. Luego, a la salida del láser se colocó un aislador óptico para evitar reflexiones que dañen el láser. Como láser se usó un modulo integrado DFB-LD de tipo FU-641SEA-1Mx de Mitsubishi de 1550 nm [44]. A la salida del mismo se colocó un modulador de intensidad (Intensity Modulator, IM) para que la intensidad de la luz siempre sea la misma. Si llega un pulso solo, ya sea $|e\rangle$ ó $|l\rangle$, el modulador de intensidad no hace nada sobre la señal pero si llegan dos pulsos juntos recorta la intensidad de ambos a la mitad. Luego hay un *phase modulator* que se utiliza para cambiar la fase relativa entre los pulsos de un mismo símbolo. Este último instrumento no fue usado durante este trabajo pero es necesario para la implementación del protocolo de QKD. Hasta este punto se sigue trabajando con luz intensa. Luego se colocó un atenuador y se pasa a tener luz de pocos fotones. Para realizar las mediciones se enviaron trenes que están compuestos por 20 pares de pulsos cada cierto tiempo.

Por otro lado para la detección de los fotones se envió la señal de salida del fotodiodo a un detector de fotones únicos para el rango cercano al infrarrojo ID Quantique 201 [45]. Al analizar las mediciones hay que tener en cuenta que el detector introduce errores en la detección de fotones debido a las cuentas de oscuridad. A su vez, luego de detectar un pulso el mismo se cierra por 20 μ s. Si durante ese tiempo llega un foton el detector no lo detecta. Cuando le llega una señal del *trigger*, este instrumento comienza a detectar durante una ventana de tiempo y manda una señal al time tagger cuando le llega un pulso. Se usó un *time tagger* de Swabian instruments [46]. El *time tagger* luego guarda el tiempo de llegada de la señal del detector,

es decir si el pulso es $|e\rangle$ ó $|l\rangle$, el número de símbolo y el número de tren. Esta información la envía a la PC. Para controlar el tiempo y decidir en que momento enviar los pulsos se usa el *trigger*. El *trigger* también le indica al *tagger* en que momento se enviaron los pulsos y así puede definir si se trata del bin *early* ó *late* y le indica al detector IDQ en que momento comenzar a medir.

La PC recibe una lista de tiempos en los que llegaron los pulsos del detector. Con esto genera un histograma del cual se obtienen la amplitud relativa del bin del medio que se usa en la implementación del lazo de estabilización de arduino descrita en la sección anterior. Se usa el primer símbolo de cada tren para estabilizar el interferómetro. Se debe recordar que al usar un símbolo para estabilizar, al estar trabajando con luz de pocos fotones, no se puede utilizar para otras mediciones. Es por esto que en el caso de luz tenue el lazo de arduino solo puede corregir cada dos segundos.

Además, en el esquema se muestra también el sistema de estabilización en temperatura. El interferómetro se encuentra dentro del gabinete de aluminio. Del lado interior de la tapa del gabinete se colocó la termocupla conectada al circuito del control de temperatura. Del lado de afuera del interferómetro, sobre la tapa, se encuentra la celda peltier junto con el disipador encima del mismo.

4.2 Caracterización del interferómetro con una fuente de pocos fotones

En esta sección se optimizó el sistema de generación y detección de pulsos. Por un lado se modificó el tiempo entre los pulsos generados Δt para calcular el valor óptimo y luego se generaron dos estados *time-bin* usando el lazo de maximización y minimización del arduino. También se simuló la interferencia de dos pares de pulsos para corroborar el comportamiento que se observa experimentalmente.

4.2.1 Optimización de generación de pulsos.

Los pulsos, de duración τ y separación ΔT , son generados usando un generador de patrones (GPP), implementado a partir de un serializador de 8 bits y un lazo PLL que genera una señal de reloj a una frecuencia F_{GPP} múltiplo de la frecuencia de la señal de entrada provista por la placa FPGA: $F_{GPP} = M * f_{FPGA}$. Para trabajar con codificación de fase, la salida del generador de patrones consiste siempre en un par de pulsos. Éstos se obtienen serializando la secuencia de 8 bits “10100000” o cualquier otra secuencia cíclica equivalente. El dispositivo “serializa”, es decir que genera la secuencia mencionada a la salida en forma secuencial, a una frecuencia F_{GPP} : entonces cada bit tiene una duración de $\frac{1}{8F_{GPP}}$. Tanto la duración de los pulsos como su separación depende de la frecuencia de serializado F_{GPP} . La forma de variar los parámetros

τ y ΔT es cambiar esta frecuencia; esto se puede hacer modificando la configuración del lazo PLL al cambiar el multiplicador entero M , o al cambiar la frecuencia de entrada provista por la FPGA. En este último caso, esto altera los retardos y tiempos de sincronización del resto de los sistemas controlados por la FPGA. Entonces se fija $F_{FPGA}=15$ MHz y se varía M en pasos discretos alrededor de $M=30$.

El tiempo de separación entre los pulsos generados, Δt , se define mediante la placa FPGA. Es posible cambiar Δt variando la frecuencia del reloj serializador del GPP, f_{GPP} . La relación entre separación de pulsos y el tiempo entre los pulsos generados es $\Delta t = \frac{1}{4f_{GPP}}$. Dado el valor de frecuencia de entrada f_{FPGA} y el rango de frecuencias prácticas del serializador, al cambiar el multiplicador M del lazo PLL en valores enteros, sólo es posible cambiar esta frecuencia en pasos de 15 MHz, que equivale a 0.07 ns. En la figura 4.2 se graficaron los histogramas del tiempo de llegada de las cuentas al detector variando la frecuencia f_{FPGA} . Como se esperaba, en cada una de las mediciones se observa acumulación de detecciones en tres bins temporales: el bin de la derecha corresponde al bin $|l\rangle$ que fue por el camino largo, el del medio es la interferencia del bin $|e\rangle$ del camino largo con el bin $|e\rangle$ que fue por el camino corto y finalmente el bin de la izquierda corresponde al bin $|e\rangle$ que fue por el camino corto. Antes de realizar el histograma se restaron las cuentas de oscuridad y se normalizó el numero de cuentas de forma que el bin de la izquierda siempre tenga intensidad 1. De esta forma es posible comparar mediciones de distinto largo ya que solo es de interés la altura relativa entre los pulsos. El valor del número de cuentas de oscuridad se obtuvo a partir de la estadística de conteo del histograma (sin normalizar) en un intervalo de tiempo alejado de los tiempos de detección de los tres pulsos. Para ello se promedió el número de cuentas con tiempo de llegada entre -5.4 ns y -3.4 ns habiendo redefinido el tiempo tal que $t = 0$ sea el tiempo de llegada del primer bin. Luego se restó este valor a la intensidad del histograma y se procedió a normalizar los datos.

En primer lugar se observa que hay una diferencia de alturas significativa entre los bins laterales, que en el caso ideal deberían tener la misma altura. La diferencia de alturas se debe a pérdidas diferenciales en alguno de los acoples de fibra en el camino largo, o una pérdida adicional impuesta por alguno de los componentes. En esta instancia esa diferencia no se corrigió ya que facilita encontrar la frecuencia óptima. Como se observa en la figura 4.2, cuando el tiempo entre los pulsos Δt no coincide con el tiempo de *delay* entre los caminos del interferómetro, el bin del medio se ensancha y tiene dos picos. Mirando los graficos se observa que la frecuencia óptima de la FPGA es 480 MHz que equivale a un $\Delta t = 2.08$ ns. Es por esto que para futuras mediciones se fijó una frecuencia de 480 MHz para el serializador del GPP, que se obtiene a partir de sintetizar esta frecuencia usando un lazo PLL sobre la señal provista por la placa FPGA de 15 MHz y un multiplicador entero $M=32$.

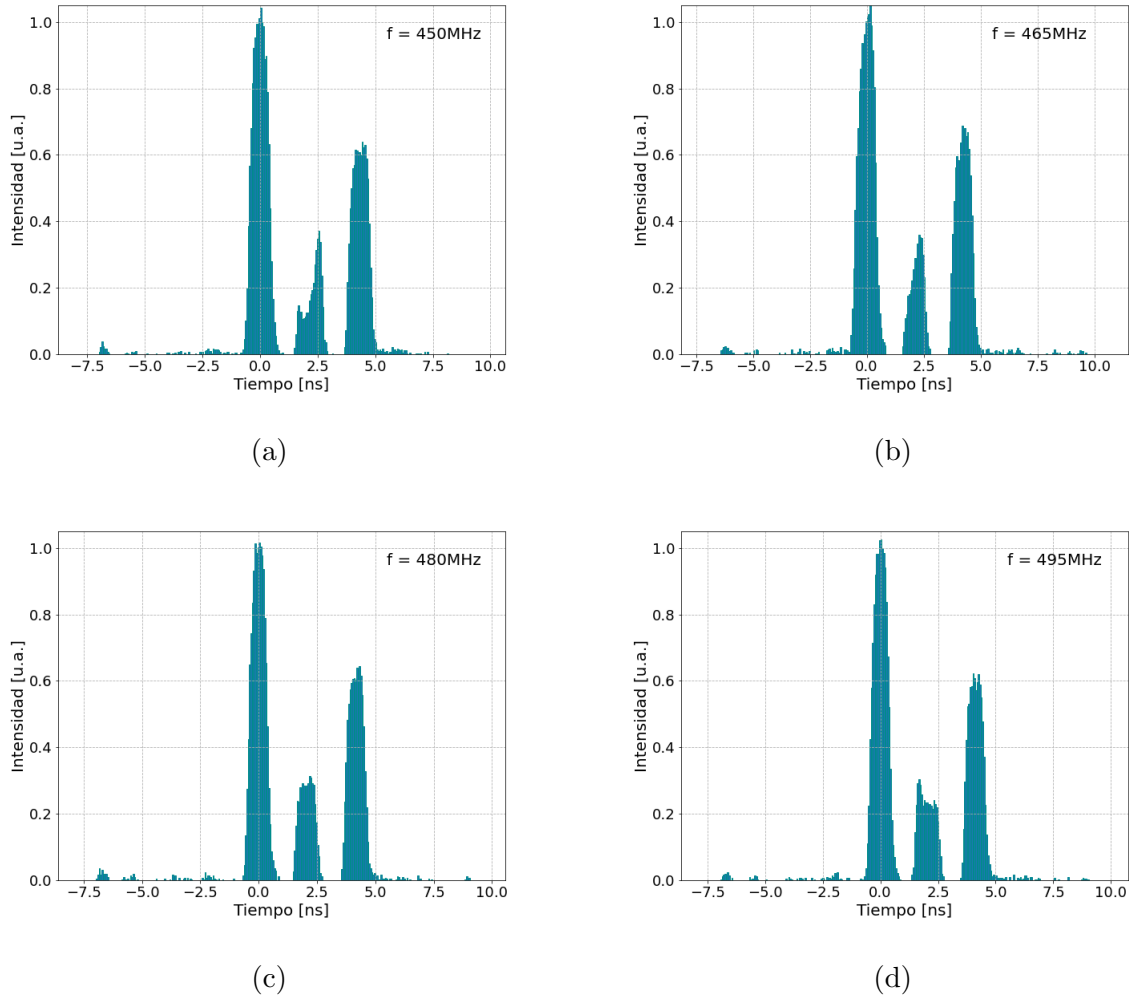


Figura 4.2: Histogramas de cuentas a la salida del interferómetro usando una fuente de luz tenue y variando la frecuencia de la FPGA que determina Δt entre los pulsos generados. Se quitaron las cuentas de oscuridad y se normalizó la intensidad. (a) Usando $f_{FPGA} = 450$ MHz que equivale a $\Delta t = 2.2$ ns. (b) Usando $f_{FPGA} = 465$ MHz ($\Delta t = 2.15$ ns). (c) Usando $f_{FPGA} = 480$ MHz ($\Delta t = 2.08$ ns). (d) Usando $f_{FPGA} = 495$ MHz ($\Delta t = 2.02$ ns).

Una vez optimizado el método de generación de pulsos se realizó una medición usando el lazo de Arduino para minimizar la interferencia. El histograma de la medición de tiempo de llegada de fotones se muestra en la figura 4.2c. Se observa que la mejor relación de contraste entre el bin central y los laterales es de 1:0.285. Esto es significativamente peor que lo que se esperaría lograr con un contraste de 0.985 como se había logrado con luz intensa. Es posible que el contraste haya cambiado ya que se está trabajando con un láser distinto. Se observa que los bins de los costados presentan una diferencia de altura significativa. Es por esto que se invirtieron las fibras a la salida del primer *splitter* del interferómetro y se repitió la medición para intentar salvar la diferencia. El resultado se muestra graficado en la figura 4.3. Se normalizó la señal de forma tal que la intensidad del bin de la izquierda valga 1. La intensidad medida del bin de la derecha es de 0.725 ± 0.025 . Se observa que se logró reducir

la diferencia de altura significativamente y simultáneamente bajar la cantidad de luz del bin de interferencia a (0.097 ± 0.013) . Podemos calcular la visibilidad máxima alcanzable a partir de la relación entre las intensidades I_1 e I_2 de los pulsos interactuantes:

$$v = \frac{2\sqrt{I_1 I_2} \gamma}{I_1 + I_2}, \quad (4.1)$$

Donde γ es una medida del grado de coherencia entre los dos haces. Asumiendo una longitud de coherencia mayor que la diferencia de caminos impuesta por el interferómetro desbalanceado, $\gamma \approx 1$ y entonces la visibilidad ideal es $v = 0.985$. Para esta visibilidad se espera una intensidad relativa mínima en el bin central de $I_{min} = 0.025$ [47].

Creemos que la limitación se debe a la longitud de coherencia del láser DFB utilizado (Mitsubishi FU641SE-A), cuyo ancho de línea es de aproximadamente 500 MHz por lo que una diferencia de camino de 40 cm comienza a afectar el grado de coherencia de ondas separadas por ese retardo. A su vez, se observaron otros efectos que no pueden ser explicados por la diferencia de intensidad.

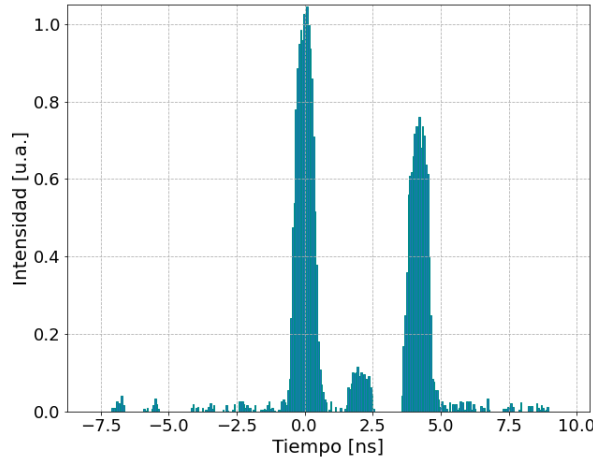


Figura 4.3: Histograma normalizado y sin cuentas de oscuridad de la salida del interferómetro de Mach-Zehnder usando una fuente de pocos fotones luego de haber invertido la fibra a la salida del primer *beam-splitter*. Se fijó un desfase de $\Delta\varphi = \pi$. La intensidad del bin de interferencia es de 0.097 ± 0.013 . El bin de la derecha tiene una intensidad de 0.725 ± 0.025 .

A continuación se muestra cómo generar otro estado desfasado 180° del anterior. Es decir que en vez de generar un mínimo de interferencia sobre la salida, se puede generar un máximo. A partir de los valores de intensidad máximo y mínimo podremos determinar la visibilidad real del interferómetro con la fuente de luz utilizada.

4.2.2 Generación de un segundo estado *time-bin*.

Se logró generar, mediante el uso del interferómetro de Mach-Zehnder y luego de la optimización de la FPGA, un estado *time-bin* con desfase $\Delta\varphi = \pi$ como se mostró en la figura 4.3. La intensidad del bin de interferencia (el del medio) en este caso es de 0.097 ± 0.013 . Luego se buscó generar otro estado *time-bin* con $\Delta\varphi = 0$. El resultado se muestra en la figura 4.4. El bin de interferencia tiene una intensidad de 3.864 ± 0.086 . Usando los resultados del máximo y mínimo valor logrado para la intensidad del bin de estabilización se obtiene que el contraste logrado para el interferómetro de Mach-Zehnder usando una fuente de luz de pocos fotones es de 0.9512 ± 0.0064 . Este contraste es mejor al hallado con luz intensa. Se observa que al cambiar el sistema para maximizar en lugar de minimizar la señal, se invierte la relación de altura entre los bins de los costados y el bin de la derecha pasa a ser mas alto que el de la izquierda. Es posible que la conformación de pulsos ópticos no sea ideal, y exista una señal de base que produce interferencia en el tercer bin y esta es constructiva o destructiva según la condición de fase impuesta por el *fiber stretcher*. En esta medición la altura del bin de la izquierda es nuevamente 1 ya que se eligió la normalización para que eso ocurra y el bin de la derecha tiene una intensidad de 1.252 ± 0.035 .

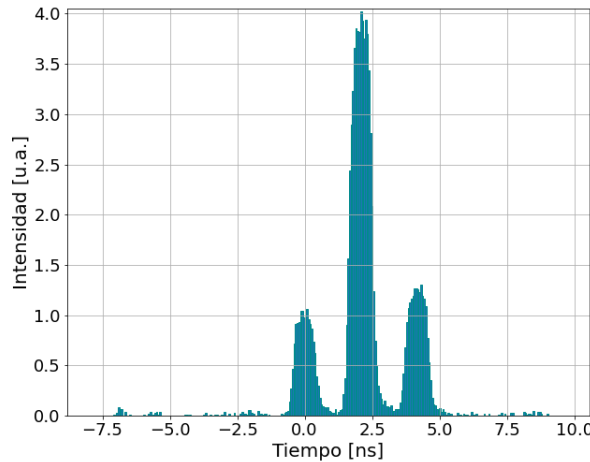


Figura 4.4: Generación de estado *time-bin* con $\Delta\varphi = 0$ usando el lazo de maximización de arduino. Intensidad del bin de estabilización lograda es 3.868 ± 0.086 . El bin de la derecha tiene una intensidad de 1.252 ± 0.035 .

Comparando los dos valores de contraste o visibilidad obtenidos; uno a partir de las intensidades de los haces interfirientes medida sobre los pulsos laterales, asumiendo coherencia mutua ideal, y el otro a partir de los valores de intensidad máxima y mínima de interferencia, podemos obtener una cota inferior para el grado de coherencia de la fuente retardada: $\gamma \approx 0.96$, por lo que podemos inferir que la coherencia del láser DFB está en el límite de lo aceptable para poder obtener buen contraste sobre un interferómetro con el retardo ensayado.

4.2.3 Simulación de pulsos *time-bin*.

Se mencionó que con una diferencia de altura del 30 % y una visibilidad de 0.985 debería ser posible lograr una interferencia menor a la hallada experimentalmente. Para corroborar esto se simuló la interferencia de dos pulsos separados un tiempo $\Delta t = 2.08$ ns, uno con una altura de 1 y otro con una altura de 0.7 al pasar por un interferómetro con visibilidad de 0.985. Por simplicidad y porque solo era de interés estudiar la altura relativa y no la forma de los pulsos se simularon los pulsos de luz como gaussianas angostas. Los pulsos simulados se muestran en la figura 4.5. En rojo se simuló el par de pulsos que va por el camino corto, y llega antes al detector, definiendo como tiempo 0 el momento en el que llega el bin $|e\rangle$ (el de la izquierda) del símbolo que viaja por el camino corto del interferómetro. Se definió la intensidad de este símbolo como 1. En azul se simuló el pulso que viajaba por el camino largo con una intensidad de 0.7.

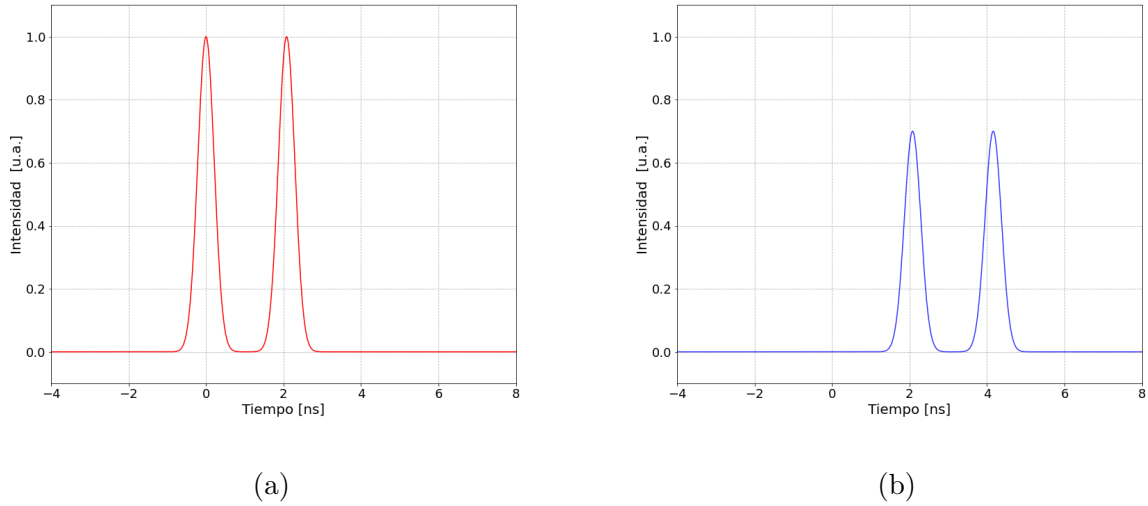


Figura 4.5: Simulación de símbolos como pulsos gaussianos angostos. (a) símbolo que viaja por el camino corto y llega antes. (b) símbolo que viaja por el camino largo y llega después.

En la figura 4.6 se graficaron los resultados de la simulación de interferencia de estos símbolos para dos desfases; $\Delta\varphi = \pi$ y $\Delta\varphi = \pi$. En la simulación del estado de *time-bin* de interferencia destructiva se llega a un mínimo de interferencia de 0.052. Para el caso de maximización de la intensidad de interferencia se obtuvo un valor de 3.35 para el bin de interferencia. La diferencia de altura hace que no sea posible llegar un mínimo absoluto como sería el caso ideal ni a un máximo de intensidad = 4. Sin embargo, no explica por qué al pasar del lazo de minimización al de maximización se invierte la altura relativa de los bins de los costados. También falla este modelo al intentar predecir el mejor máximo hallado ya que fue posible lograr experimentalmente un máximo de interferencia de 0.386 ± 0.0064 , significativamente mayor al valor predicho en la simulación de 3.35.

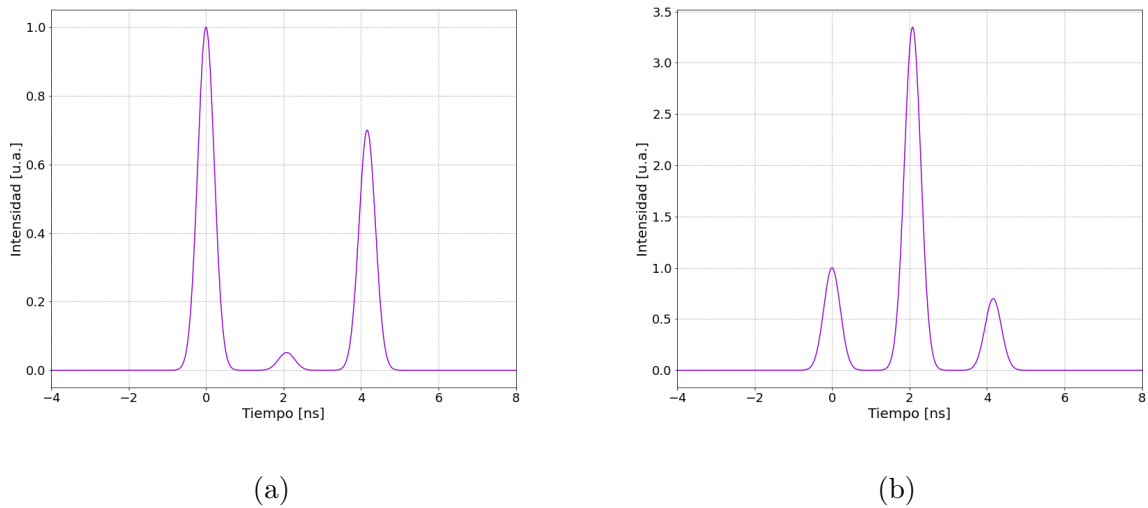


Figura 4.6: Simulación de interferencia de símbolos como pulsos gaussianos angostos. (a) Desfasaje $\Delta\varphi = \pi$, la intensidad del bin del medio es de 0.052. (b) Desfasaje $\Delta\varphi = 0$, intensidad del bin de interferencia es de 3.35.

Recordando que se observó que al cambiar entre minimizar y maximizar la interferencia, la altura relativa de los bins de los costados se invirtió; el bin de la derecha se vuelve más alto que el de la izquierda, se modificó el modelo de la simulación, para incluir una señal base o “fantasma” posterior al patrón de par de pulsos, que genera interferencia. Si no interfiriese se hubiese sumado a los tres picos y por ende hubiese sido eliminado cuando se quitaron las cuentas de oscuridad. Para corroborar si este modelo se ajusta a lo observado se simuló nuevamente la interferencia de los símbolos, pero en lugar de imponer una diferencia de altura entre ellos se tomó la intensidad de ambos como 0.9 y se sumó una intensidad de base que comienza luego del primer pulso y que tiene una altura de 0.1. Se eligió este valor para la base tal que la diferencia de alturas producida sea similar a la hallada experimentalmente. En este caso simulando con visibilidad 0.985, el bin central llegaba a valores de intensidad menor (mayor) a lo obtenido experimentalmente para el lazo de minimización (maximización) por lo que en este caso se simuló con visibilidad de 0.935 para a cual se obtienen alturas más razonables. Resulta razonable cambiar el contraste en este caso ya que se observó experimentalmente que el contraste cambia al pasar de luz intensa a luz de pocos fotones. Los resultados se muestran en la figura 4.7, donde se define el tiempo de llegada del primer bin como 0. Se simula en función del tiempo de llegada al detector, por lo que el bin de la izquierda es el bin $|e\rangle$ que viaja por el camino corto y el de la derecha es el bin $|l\rangle$ que viaja por el largo.

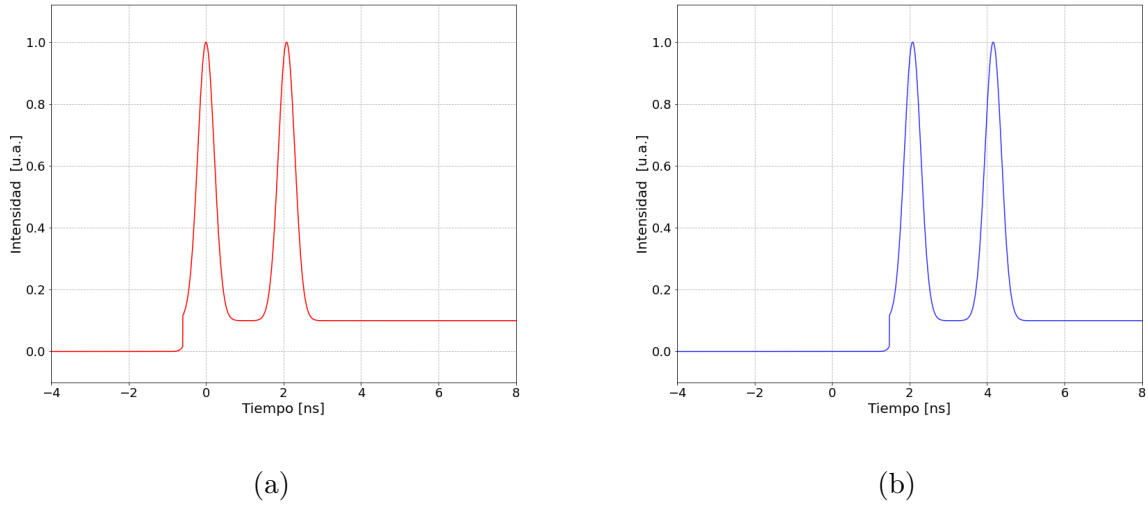


Figura 4.7: Simulación de símbolos con intensidad total 1 con una señal de base que comienza con el primer bin de una altura de 0.1. (a) Símbolo que viaja por el camino corto y llega antes. (b) símbolo que viaja por el camino largo y llega después.

A continuación en la figura 4.8 se muestra la interferencia simulada de estos pulsos. Se observa que la altura relativa de los pulsos de los costados se invierte cambiar la condición del protocolo de estabilización ($\varphi = 0$ o $\varphi = \pi$). Fijando la intensidad del primer bin a 1 se obtiene que el bin de la derecha tiene una intensidad de 0.969 para $\Delta\varphi = \pi$ y de 1.368 para $\Delta\varphi = 0$. Este modelo de pulsos con una base reproduce de forma adecuada la intensidad de los pulsos de interferencia y la altura relativa de los pulsos laterales.

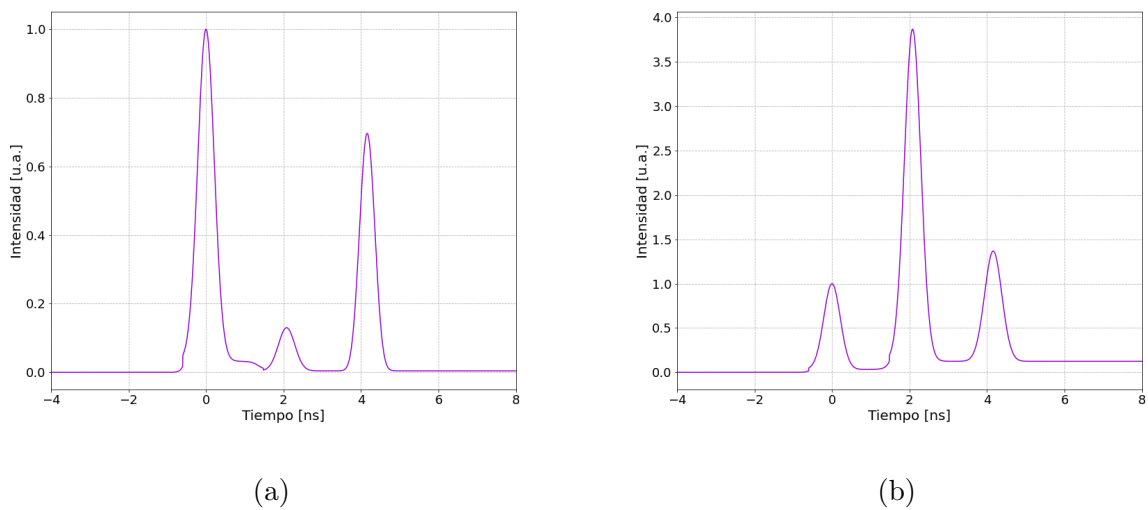


Figura 4.8: Simulación de interferencia de los símbolos (a) $\Delta\varphi = \pi$, el bin de interferencia tiene una intensidad de 0.13. (b) $\Delta\varphi = 0$ donde el bin del medio tiene una intensidad de 3.87.

Luego de obtener estos resultados se buscó verificar experimentalmente si la señal de en-

trada al interferómetro tenía una base que comenzaba luego del primer pico. Se observó que la señal eléctrica que envía la placa GPP al láser ya presenta una diferencia en las amplitudes de pico de cada uno de los pulsos, pero mucho menor a la observada en los histogramas por lo que no es la causa de la diferencia de altura del primer y último bin. También se observó la salida del interferómetro, iluminado con luz intensa pero enviando dos pulsos. Se observó que si sólo se envía el pulso *late* (el de la derecha en la figura 4.7) y luego se le agrega el pulso *early* (el de la izquierda) aumenta la altura del bin de la derecha, el bin *late*. Por otro lado, si se envía un pulso *early* y luego se agrega el pulso *late*, la altura del primer pulso no se modifica. Esto indica que cada pulso al ser emitido genera una señal parásita que lo acompaña, y que entonces hay un fondo de luz correlacionado que aparece posteriormente a la emisión de este pulso. Resulta entonces razonable concluir que lo que ocurre es que se obtiene una base en cada señal que interfiere con el pulso siguiente y con la señal de base de este otro pulso, provocando una cota inferior para el mínimo de 0.13.

Otro detalle a destacar con respecto al experimento con una fuente de pocos fotones es que el contraste cambia cuando se trabaja con luz intensa ó con luz de pocos fotones. Creemos que este fenómeno se debe a un efecto de birrefringencia térmica, inducida por la luz intensa. Al enviar luz intensa, la misma puede calentar la fibra y modificar así la polarización relativa de ambos caminos. Si bien el efecto es reversible, ya que puede ser compensado modificando el estado de polarización con el controlador de polarización manual, presenta un problema, ya que para maximizar el contraste se hace un barrido de la fase mientras se cambia la polarización de uno de los caminos moviendo el controlador manual de polarización. Esta optimización resulta más compleja de realizar en luz tenue, ya que es preciso acumular detecciones en cierta cantidad de tiempo para disponer de una estadística poco dispersa. Este es un método menos exacto que el que se usa con luz intensa donde se mide la intensidad a la salida del interferómetro con el osciloscopio.

Capítulo 5

Conclusiones

En el presente trabajo se buscó estabilizar en temperatura un interferómetro de Mach-Zehnder para la implementación experimental de protocolo de QKD codificado en *time-bin* implementado en fibra óptica. Para la preparación de los estados se usó un láser de 1550 nm. Se generaron dos pulsos de luz usando una señal eléctrica controlada por medio de una FPGA y una placa GPP. Para la detección se usó un interferómetro de Mach-Zehnder.

En primer lugar se buscó estudiar la estabilidad del láser utilizado como fuente del interferómetro. Se usó un láser ITLA Pure Photonics que cuenta con dos modos de operación: modo *whisper* y modo *dither*. En el modo *whisper* se deshabilitan los lazos de control, en la medida de lo posible, por lo que la frecuencia del láser es más estable. Este fue el modo de preferencia que se utilizó durante este trabajo. En una primera instancia se buscó caracterizar las fluctuaciones de la frecuencia del láser con un analizador de espectros O.S.A. pero se observó que éstas estaban por debajo de la resolución del instrumento. Debido a esto se cambió la forma de estudiar la estabilidad del láser. Para ello se midió la frecuencia de batidos entre dos fuentes idénticas y se encontró que por tiempos de hasta 30 s esta frecuencia se mantuvo estable.

Una vez caracterizada la fuente de luz se estudió la estabilidad del interferómetro de Mach-Zehnder en fibra óptica con una fuente de luz intensa. Primero se comparó las fluctuaciones de la interferencia con y sin desbalance de caminos. Se observó que en el caso del interferómetro balanceado ($\Delta L = 0$) el interferómetro resulta más estable que cuando se introduce un desbalance de caminos de $\Delta L = 40$ cm. Para el interferómetro desbalanceado se observó que en una medición de 35 minutos la fase fluctuó 21 ciclos, lo que equivale a un cambio en temperatura de 4 °C. A su vez, con el interferómetro balanceado fue posible conseguir un contraste $c = (1.000 \pm 0.011)$ mientras que con el interferómetro desbalanceado el mejor contraste logrado fue $c = (0.985 \pm 0.013)$.

Sobre el interferómetro también se utilizó un lazo de control conformado por un Arduino Mega junto con el *fiber stretcher* para estabilizar la fase relativa. Con este lazo de estabilización se logró mantener estable el interferómetro durante mediciones de 50 minutos, con fluctuaciones

por debajo del 10%. Usando este lazo también es posible realizar un barrido de la fase para calcular el contraste. Usando esto se midió el contraste en dos condiciones de temperatura y se encontró que el contraste varía al subir la temperatura. Si bien el lazo de estabilización es capaz de compensar las fluctuaciones de fase con la temperatura, ya que es posible mantener constante la fase para tiempos largos, sigue siendo necesario estabilizar en temperatura del interferómetro para que no cambie el contraste del mismo.

Una vez caracterizadas las fluctuaciones del interferómetro de Mach-Zehnder en temperatura se diseñó y construyó un control de temperatura basado en el componente MAX1979. También se construyó un gabinete contenedor de aluminio dentro del cual se colocó el interferómetro. El control de temperatura funciona por medio de un lazo PID. Utiliza un termistor para sensar la temperatura dentro del gabinete y una Peltier para enfriarlo. Una vez construido el control de temperatura se caracterizó su funcionamiento. Se encontró que se puede modelar la relación entre la temperatura y la resistencia del termistor (R_T) usando la ecuación de Steinhart & Hart. Se calcularon los coeficientes A y B de la ecuación a partir de un ajuste de los resultados experimentales. Se obtuvo $A = (1.53 \pm 0.20) \times 10^{-3}$ y $B = (1.97 \pm 0.22) \times 10^{-4}$. Dado que el coeficiente C se incluyó en la ecuación para modelar el comportamiento a grandes temperaturas y las mediciones fueron realizadas para temperaturas entre 10 °C y 40 °C, se tomó $C = 0$ en el ajuste. A su vez, se modeló por una lineal la relación entre la temperatura (T) y el voltaje monitor V_{mon} de la placa. A partir de las mediciones se obtuvo la siguiente relación: $T = (12.3 \pm 1.4) K/V V_{mon} + (280.6 \pm 1.6) K$. Una vez caracterizado el control de temperatura se lo utilizó para estabilizar la temperatura del interferómetro y se logró estabilizar el sistema con fluctuaciones debajo de 50 mK, que se considera satisfactorio.

Finalmente se utilizó el interferómetro de Mach-Zehnder para la implementación de un protocolo de generación y detección de pulsos *time-bin* donde se utiliza luz de pocos fotones. Para ello se generaron dos pulsos de luz con un láser Mitsubishi de 1550 nm (distinto al utilizado en las mediciones previas), y luego se atenúo la señal con moduladores de intensidad para obtener luz de pocos fotones. Para generar los pulsos de luz se enviaron dos pulsos eléctricos al láser usando una FPGA en conjunto con una placa GPP. Primero se buscó optimizar el mecanismo de generación de pulsos. Se buscó la frecuencia f_{GPP} , de la placa GPP, óptima que genere dos pulsos con una separación temporal Δt equivalente al retardo producido por el desbalance de caminos del interferómetro. Se obtuvo que para el interferómetro con $\Delta L = 40$ cm, la frecuencia óptima es $f_{GPP} = 480$ MHz. Luego, se utilizó el interferómetro de Mach-Zehnder para generar dos estados *time-bin* con fase $\varphi = 0$ y $\varphi = \pi$ a modo de demostración de la capacidad de control de fase relativa. Cada par de pulsos se divide en dos a la entrada del interferómetro y se recombinan interfiriendo a la salida del mismo. En la entrada del interferómetro ingresa un pulso compuesto por dos bins que en su conjunto conforman un *qubit*, y a la salida del interferómetro se observan tres *bins*. La información respecto el estado de *qubit* se encuentra en el bin central.. Se logró generar ambos estados variando la condición de

estabilización del lazo de control. Usando las intensidades relativas de los estados medidos a la salida del interferómetro se calculó el contraste del interferómetro en el marco de luz tenue obteniendo $c = (0.9512 \pm 0.0064)$. Al variar la fuente entre luz intensa y luz de pocos fotones se observó que el contraste del interferómetro cambia debido a efectos de birrefringencia térmica inducida por la luz intensa. Otro efecto que se observó fue que al cambiar el lazo para pasar de $\varphi = 0$ a $\varphi = \pi$, la altura relativa entre los *bins* laterales se invierte. Se postuló que los pulsos contienen una base de luz parásita que aparece luego de cada pulso, que interfieren y causan la diferencia de altura. Se simuló la interferencia de los pulsos para estimar si esta hipótesis es suficiente para explicar la diferencia de altura observada y se concluyó que lo es.

Bibliografía

- [1] Simon Singh. *The Code Book: How to Make It, Break It, Hack It, Crack It*. Delacorte Press, 2001.
- [2] Friedrich Kasiski. *Die Geheimschriften und die Dechiffrier-Kunst*. E. S. Mittler und Sohn, 1863.
- [3] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, February 1 2008. Submitted to Reviews of Modern Physics.
- [4] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 2018.
- [5] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.
- [6] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.
- [7] Steven M Bellovin. Frank miller: Inventor of the one-time pad. *Cryptologia*, 35(3):203–222, 2011.
- [8] G. S. Vernam. Secret signaling system, July 1919.
- [9] Agustina G. Magnoni. Distribución cuántica de claves en aire con estados señuelo. Tesis de licenciatura en ciencias físicas, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, septiembre 2024.
- [10] J. P. Paz, F. Cerisola, A. J. Roncaglia, and C. T. Schmiegelow. *Versión preliminar del libro Física Cuántica*. 2022.
- [11] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, Bangalore, India, December 9–12 1984.
- [12] Won-Young Hwang. Quantum key distribution with high loss: toward global secure communication. *Physical review letters*, 91(5):057901, 2003.
- [13] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical review letters*, 94(23):230504, 2005.

- [14] Evan Meyer-Scott, Christine Silberhorn, and Alan Migdall. Single-photon sources: Approaching the ideal through multiplexing. *Review of Scientific Instruments*, 91(4):041101, 04 2020.
- [15] Artur K Ekert. Quantum cryptography based on bell’s theorem. *Physical review letters*, 67(6):661, 1991.
- [16] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301–1350, 2009.
- [17] Julián Morales. Estabilización activa de un interferómetro de fibra óptica para comunicaciones cuánticas con codificación en estados time-bin. Master’s thesis, Universidad de Buenos Aires, Facultad de Ciencias Exactas y Naturales, Departamento de Física, Buenos Aires, Argentina, 2020.
- [18] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin. Distribution of time-bin entangled qubits over 50 km of optical fiber. *Physical Review Letters*, 93(18), October 2004.
- [19] Ignacio H. López Grande. *Distribución cuántica de claves criptográficas: Experimentos y tecnologías*. PhD thesis, Universidad de Buenos Aires, Facultad de Ciencias Exactas y Naturales, Departamento de Física, Buenos Aires, Argentina, December 2018. Tesis Doctoral. Director: Dr. Miguel A. Larotonda, Consejero de Estudios: Dr. Claudio Iemmi. Lugar de Trabajo: Laboratorio de Óptica Cuántica (DEILAP-CITEDEF).
- [20] Cristiano Pendão and Ivo Silva. Optical fiber sensors and sensing networks: overview of the main principles and applications. *Sensors*, 22(19):7554, 2022.
- [21] Weimin Lyu, Shuyang Chen, Fengze Tan, and Changyuan Yu. Vital signs monitoring based on interferometric fiber optic sensors. *Photonics*, 9(2), 2022.
- [22] Xixi Li, Dejun Liu, Rahul Kumar, Wai Pang Ng, Yong qing Fu, Jinhui Yuan, Chongxiu Yu, Yufeng Wu, Guorui Zhou, Gerald Farrell, Yuliya Semenova, and Qiang Wu. A simple optical fiber interferometer based breathing sensor. *Measurement Science and Technology*, 28(3):035105, feb 2017.
- [23] Kunjian Cao, Yi Liu, and Shiliang Qu. Compact fiber biocompatible temperature sensor based on a hermetically-sealed liquid-filling structure. *Opt. Express*, 25(24):29597–29604, Nov 2017.
- [24] Shu na Wang, Ri qing Lv, Yong Zhao, and Jun kai Qian. A mach-zehnder interferometer-based high sensitivity temperature sensor for human body monitoring. *Optical Fiber Technology*, 45:93–97, 2018.
- [25] D. W. Allan. Statistics of atomic frequency standards. *Proceedings of the IEEE*, 54(2):221–230, Feb 1966.

- [26] Marcelo Alejandro Luda. *Instrumentación y control con aplicaciones en óptica y metrología*. PhD thesis, Universidad de Buenos Aires, 2021.
- [27] Ron Beard and Ken Senior. Clocks. In *Springer Handbook of Global Navigation Satellite Systems*, pages 121–164. Springer International Publishing, 2017. (see p. 17).
- [28] Pure Photonics. Pure photonics - unleash the power of tunable lasers, 2024. Accessed: 2024-09-03.
- [29] X. Zhang, F. Xie, M. Chen, and Y. Yang. A highly stable frequency single-mode optical fiber laser based on a fabry-perot etalon. *Optical Fiber Technology*, 73,103047, 2022.
- [30] Pure Photonics. Tunable laser technology. <https://purephotonics.com/tunable-laser-technology/>, 2024. Accessed: 2024-08-27.
- [31] Pure Photonics. Low noise tunable laser, clean light portfolio - feature guide.
- [32] Burleigh Instruments, Inc. *Burleigh WA-1000/WA-1500 Wavemeter® Laser Wavelength Meters Instruction Manual*, 1997. Instruction Manual.
- [33] Rigol Technologies. *DSA800 Series Spectrum Analyzers Manual*. Accessed: 2024-09-05.
- [34] International Telecommunication Union. Fibra óptica monomodo normalizada ITU-T G.652.D - 1310/1550nm. Recommendation G.652.D, ITU-T, November 2016.
- [35] Thorlabs. Fiber Coupler 10202A-50-FC, 2023. Accessed: 2024-09-14.
- [36] IDIL Fibres Optiques. IDIL Fiber Stretcher. Accessed: 2024-09-14.
- [37] Arduino. Arduino Mega 2560 Rev3. Accessed: 2024-09-14.
- [38] G. B. Hocker. Fiber-optic sensing of pressure and temperature. *Applied Optics*, 18(9):1445–1448, 1979.
- [39] T. S. Priest, K. T. Jones, G. B. Scelsi, and G. A. Woolsey. Thermal coefficients of refractive index and expansion in optical fibre sensing. In *Proceedings of the 12th International Conference on Optical Fiber Sensors*, volume 16 of *OSA Technical Digest Series*, Washington, D.C., 1997. Optical Society of America, Optical Society of America. Reprinted with permission from OSA. © 1997 OSA.
- [40] T. Baak. Thermal coefficient of refractive index of optical glasses. *Journal of the Optical Society of America*, 59:851–857, 1969.
- [41] Maxim Integrated. *Integrated Temperature Controllers for Peltier Modules (MAX1979)*, 2005. Accessed: 2024-09-22.
- [42] Omega Engineering. Pid controllers. Accessed: 2024-09-22.

- [43] John S. Steinhart and Stanley R. Hart. Calibration curves for thermistors. *Deep-Sea Research and Oceanographic Abstracts*, 15(4):497–503, August 1968.
- [44] MITSUBISHI (Dispositivos Ópticos). *Módulo Integrado DFB-LD con Modulador EA FU-641SEA-1Mx 1.55 mm (Paquete de 7 Pines con Conector K, Aplicación Digital de 10GB/s)*. Manual de usuario.
- [45] ID Quantique. *Detector de Fotón Único Serie id201 para el Infrarrojo Cercano*, n.d. Manual de usuario.
- [46] Swabian Instruments. *Manual de Usuario de Time Tagger, Versión 2.9.0.0*, Junio 2021. Manual de usuario.
- [47] Eugene Hecht. *Óptica*. Addison Wesley, Madrid, tercera edición edition, 1998.

Tesis disponible bajo Licencia Creative Commons

Atribución – No Comercial – Compartir Igual (by-nc-sa) 2.5 Argentina

Buenos Aires, 2024